

Determinants of Subquotients of Galois Representations Associated to Abelian Varieties

Eric Larson and Dmitry Vaintrob

Abstract

Given an abelian variety A of dimension g over a number field K , and a prime ℓ , the ℓ^n -torsion points of A give rise to a representation $\rho_{A,\ell^n} : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$. In particular, we get a *mod- ℓ representation* $\rho_{A,\ell} : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_{2g}(\mathbb{F}_\ell)$ and an *ℓ -adic representation* $\rho_{A,\ell^\infty} : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_{2g}(\mathbb{Z}_\ell)$. In this paper, we describe the possible determinants of subquotients of these two representations. These two lists turn out to be remarkably similar.

Applying our results in dimension $g = 1$, we recover a generalized version of a theorem of Momose on isogeny characters of elliptic curves over number fields, and obtain, conditionally on the Generalized Riemann Hypothesis, a generalization of Mazur's bound on rational isogenies of prime degree to number fields.

1 Introduction

Let A be a g -dimensional abelian variety over a number field K . The *ℓ -adic Tate module*

$$A[\ell^\infty] := \varprojlim_n A[\ell^n]$$

is the limit of ℓ -power torsion points over \overline{K} . It is a \mathbb{Z}_ℓ -lattice with action by the Galois group $G_K := \text{Gal}(\overline{K}/K)$, and is one of the fundamental examples of a Galois representation.

We study in this paper one-dimensional Galois characters which can arise from these representations. Namely, we consider determinants of subquotients of the ℓ -adic Tate module of A with scalars extended from \mathbb{Z}_ℓ to either ℓ -adic fields or finite fields \mathbb{F}_{ℓ^n} . Any such determinant character with values in a field k appears after extending scalars all the way to \overline{k} . Hence studying these determinant characters with scalars extended to $\overline{\mathbb{Q}_\ell}$ gives all such characters with values in an ℓ -adic field, and extending scalars to $\overline{\mathbb{F}_\ell}$ gives all such characters with values in \mathbb{F}_{ℓ^n} .

If V is a representation of a group G over a field k , we say that $\psi : G \rightarrow \overline{k}^\times$ is an *associated character* of degree d of V if there is a d -dimensional subquotient W of $V \otimes_k \overline{k}$ such that $\psi = \det_{\overline{k}} W$. We call our principal objects of study — the associated characters of $A[\ell^\infty] \otimes \mathbb{Q}_\ell$ and $A[\ell^\infty] \otimes \mathbb{F}_\ell = A[\ell]$ — the *ℓ -adic* and *mod- ℓ* associated characters of A respectively.

The study of associated characters of these kinds goes back to Serre’s foundational work on the Open Image Theorem, which states that for an elliptic curve E without complex multiplication, the action of the absolute Galois group of a number field on the adèlic Tate module $H_1(E, \widehat{\mathbb{Z}}) = \prod_{\ell} E[\ell^{\infty}]$ is open (i.e. has finite index) in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. This is proved in two principal steps. First, in [16], Serre shows that the ℓ -adic image $\rho_{E, \ell^{\infty}}: G_K \rightarrow \mathrm{GL}_2(\mathbb{Z}_{\ell})$ has finite index for all ℓ . Second, in [17], Serre shows that for sufficiently large primes, the mod- ℓ image $\rho_{E, \ell}: G_K \rightarrow \mathrm{GL}_2(\mathbb{Z}_{\ell})$ is surjective. In each case, the proof consists of reducing the problem to the study of the ℓ -adic and mod- ℓ associated characters of E respectively, i.e. studying the Galois action on the 1-dimensional subquotients.

A major conjecture, which is still open, is whether the index of the image of G_K in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ in Serre’s theorem is bounded *uniformly* in E . The first step towards this result, for $K = \mathbb{Q}$, is Mazur’s seminal theorem on isogenies [9]. This theorem is equivalent to the statement that, for an elliptic curve E over \mathbb{Q} and for a prime $\ell > 163$, the ℓ -torsion module $E[\ell]$ is irreducible (equivalently, no isogenies $E \rightarrow E'$ defined over \mathbb{Q} have kernel of order ℓ). An essential step of Mazur’s proof is to analyze the possible associated characters (up to torsion of small degree) of subquotients of $E[\ell]$, and show that for $\ell > 163$ the list of possible associated characters is empty.

Momose in [13] gives an exhaustion (i.e. a list containing all possibilities, perhaps with excess) for the mod- ℓ associated characters of elliptic curves over number fields K attached to subquotients of $E[\ell]$, for ℓ sufficiently large depending on K . When K is quadratic, either real, or imaginary of class number greater than one (i.e. as long as $K \neq \mathbb{Q}[\sqrt{D}]$ for $D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$), the list of possible associated characters is empty. In particular, any elliptic curve E over such a quadratic field K has irreducible torsion module $E[\ell]$ (equivalently, admits no ℓ -isogenies) as long as $\ell > C_K$ for some constant C_K that depends only on K .

The main theorem of our paper gives an analogous exhaustion for abelian varieties of dimension g over K . When applied to elliptic curves, we obtain slightly stronger versions of the above results of Momose (see Theorem 1 and Corollary 2 below). While it is hopeless to classify all proper subquotients of $A[\ell]$ for $g > 1$ (for A decomposable, for example, this would involve classifying all Galois representations coming from elliptic curves), giving a complete characterization of their determinants is a more manageable task — and this is the question we study in this paper.

Serre’s Open Image Theorem is the beginning of a larger story about the Galois representations $A[\ell]$. By Faltings’ Finiteness Theorem [4] (applied to both A and $A \times A$), we know that if $\mathrm{End}_K(A) = \mathbb{Z}$, then the representations $A[\ell]$ are absolutely irreducible for ℓ larger than some constant depending on A . As with Serre’s theorem, conjecturally there should exist a uniform bound. Our main result implies this conjecture for a large class of fields, conditionally on the Generalized Riemann Hypothesis (GRH). Since our main result holds for arbitrary g , there is hope that it gives a step towards this conjecture in general.

Our paper consists of two main parts. First we study ℓ -adic associated characters of abelian varieties, giving an essentially complete classification. Then, we turn to the study

of mod- ℓ characters. We show that for ℓ greater than some constant depending only on K and g , any mod- ℓ associated character of a g -dimensional abelian variety defined over K belongs to a small list of possibilities. An abelian variety with a mod- ℓ associated character does not necessarily have an ℓ -adic associated character; therefore, a priori, there could be many more possibilities for mod- ℓ associated characters than for ℓ -adic associated characters. Remarkably, this is not the case: *Our list of possible mod- ℓ characters is closely related to the list of ℓ -adic associated characters that can occur.*

Now we will turn to a precise formulation of our results. The relationship between ℓ -adic and mod- ℓ associated characters discussed above is particularly sharp in dimension $g = 1$ (elliptic curves), especially if one assumes GRH. In this case we have the following theorem.

Theorem 1 (Theorem 6.4). *Let K be a number field. Then, there exists a finite set S_K of prime numbers depending only on K such that, for a prime $\ell \notin S_K$, and an elliptic curve E over K for which $E[\ell] \otimes \overline{\mathbb{F}}_\ell$ is reducible with degree 1 associated character ψ , one of the following holds.*

1. *There exists a CM elliptic curve E' , which is defined over K and whose CM-field is contained in K , with an ℓ -adic degree 1 associated character whose mod- ℓ reduction ψ' satisfies:*

$$\psi^{12} = (\psi')^{12} \tag{1}$$

2. *The Generalized Riemann Hypothesis fails for $K[\sqrt{-\ell}]$, and*

$$\psi^{12} = \text{cyc}_\ell^6, \tag{2}$$

where cyc_ℓ is the cyclotomic character. (Moreover, in this case we must have $\ell \equiv 3 \pmod{4}$ and the representation $\rho_{E,\ell}$ is already reducible over \mathbb{F}_ℓ .)

Remark 1.1. The proof of Theorem 1 implies that E' depends only on E (and not on ℓ); moreover, $\psi' \otimes \psi^{-1}$ is ramified only at primes of bad additive reduction for E .

The proof of Theorem 1 also shows that the set S_K is effectively computable. In Theorem 7.9, we give an explicit bound on the value of $\prod_{\ell \in S_K} \ell$.

In Case 1 of the theorem (which is the only possible case if we assume GRH), the twelfth powers of the other associated characters of $E[\ell]$ and $E'[\ell]$ also coincide, since the two representations $E[\ell]$ and $E'[\ell]$ have the same determinants (both equal to cyc_ℓ). In particular, equation (1) can be formulated more concisely as

$$\Psi^{12}(E[\ell]) = \Psi^{12}(E'[\ell]),$$

where Ψ^n is the Adams operation on the Grothendieck ring of representations of G_K over \mathbb{F}_ℓ . Similarly, we can rewrite equation (2) as $\Psi^{12}(E[\ell]) = \text{cyc}_\ell^6 \oplus \text{cyc}_\ell^6$.

Theorem 1 implies the following result. (This is also a straightforward consequence of the results of [10] and [13], but does not appear to be written anywhere in the literature.)

Corollary 2 (Corollary 6.5). *Under GRH, the degrees of prime degree isogenies of elliptic curves over K are bounded uniformly if and only if K does not contain the Hilbert class field of an imaginary quadratic field F (i.e. if and only if there are no elliptic curves with CM defined over K).*

Theorem 1 follows from the more general Theorem 4, which gives an analogous statement for arbitrary abelian varieties. Before formulating it, we need to introduce some technical notions. First, however, we give a statement in the case where K has a real embedding, which is considerably simpler. More generally, it suffices to assume that K does not contain any *CM-fields*, i.e. totally imaginary quadratic extensions of totally real fields.

Corollary 3 (Corollary 5.18). *Let K be a number field that does not contain any CM-fields (which is in particular true when K has a real embedding), and g and d be positive integers. There exists a finite set $S_{K,g}$ of prime numbers depending only on K and g , and a constant $0 < c_g < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g -dimensional abelian variety A with a mod- ℓ associated character ψ of degree d ,*

$$\psi^{2w} = \text{cyc}_\ell^{aw},$$

where a is an integer with $0 \leq a \leq 2d$, and $w = \frac{\text{lcm}(c_g, N)}{2}$ for some positive $N \leq \binom{2g}{d}$.

In general, we will try to relate the associated character ψ to the mod- ℓ reduction of an ℓ -adic associated character of another abelian variety B . This encompasses the above case, because the determinant of the entire Tate module gives an ℓ -adic associated character which is a power of the cyclotomic character, and there are no ℓ -adic associated characters of abelian varieties defined over such fields K besides twists of powers of the cyclotomic character. In order to do this, we will need to study the ℓ -adic associated characters of abelian varieties first.

Using a theorem of Faltings [4], we will see that any ℓ -adic associated character arises from an abelian variety B which has (generalized) *complex multiplication*, i.e. has action by an order in a field F , where F is a CM-field or $F = \mathbb{Q}$. Note that we do *not* assume that $\deg F = 2 \cdot \dim A$ (as is the case in the classical theory of complex multiplication); if this is the case, we call it *full* CM.

Suppose that B is an abelian variety over K with complex multiplication by a CM field F , i.e. with an injection $F \hookrightarrow \text{End}(B) \otimes \mathbb{Q}$. Then $B[\ell^\infty] \otimes \mathbb{Q}_\ell$ is an $(F \otimes \mathbb{Q}_\ell)$ -module, which one can show is free of dimension $\frac{2g}{[F:\mathbb{Q}]}$. The problem of finding ℓ -adic associated characters for the F -eigenspaces reduces to computing the $(F \otimes \mathbb{Q}_\ell)$ -determinant of this representation — composing this determinant with various embeddings $F \hookrightarrow \overline{\mathbb{Q}_\ell}$ gives these ℓ -adic associated characters of B . By the local characterization of such determinants in Appendix A (written by Brian Conrad), we see that these characters are determined (up to twists) by the CM type of B , i.e. the isomorphism class of the K - F bimodule $\Phi = \text{Lie}(B)$;

they can be described quite explicitly in terms of “algebraic” class field theoretic characters of the type studied by Serre in [16].

Specifically, given a CM type (F, Φ) we define a field $K_{F, \Phi}$ and a Galois character $\psi_{F, \Phi}: G_{K_{F, \Phi}} \rightarrow \overline{\mathbb{Q}}_\ell^\times / \mu_F$ (where μ_F is the group of roots of unity contained in F), which are uniquely determined by the following properties, as shown in Theorems 3.6 and 3.11. (Technically, the character $\psi_{F, \Phi}$ depends on a choice of embedding $\sigma: F \hookrightarrow \overline{\mathbb{Q}}_\ell$ as well, but we will usually suppress this and assume we have chosen an appropriate embedding.)

1. If an abelian variety B over K has CM of type (F, Φ) which is defined over K , then $K_{F, \Phi}$ is contained in the ground field K .
2. In the above case, the associated characters of the F -eigenspaces of $B[\ell^\infty] \otimes \mathbb{Q}_\ell$ define characters $\psi_{B, \sigma}: G_K \rightarrow \overline{\mathbb{Q}}_\ell^\times$ (indexed by embeddings $\sigma: F \hookrightarrow \overline{\mathbb{Q}}_\ell$), and modulo the group μ_F of roots of unity in F , these characters coincide with the restriction of $\psi_{F, \Phi}$ to G_K , i.e.

$$\psi_{F, \Phi}|_{G_K} \equiv \psi_{B, \sigma} \pmod{\mu_F}.$$

3. The field $K_{F, \Phi}$ is the *separating field* (i.e. minimal field of definition of the geometrically irreducible components) of the Shimura variety for some nonempty collection of polarized abelian varieties with CM type (F, Φ) .

The Shimura variety in condition 3 is the coarse moduli space for this collection of polarized abelian varieties. In particular, if the CM type (F, Φ) corresponds to an abelian variety B with full CM, then B and its CM are defined over K , since the Shimura variety is zero-dimensional in this case.

Now we can state our result for abelian varieties of arbitrary dimension g . Roughly speaking, we show that there exists an effectively computable finite set $S_{K, g}$ such that for $\ell \notin S_{K, g}$ and ψ a mod- ℓ associated character of a g -dimensional abelian variety, ψ^a is equal (mod ℓ) to a character $\psi_{F, \Phi}^b$ corresponding to a CM type (F, Φ) with separating field $K_{F, \Phi}$ contained in K , for some exponents $a > 0$ and $b \geq 0$. The exponents a and b , and the dimension $\dim_K \Phi$ of abelian varieties of CM type (F, Φ) are both bounded by a constant depending only on g and satisfy some additional restrictions.

In equation (1), the exponents a and b satisfy $a = b = 12$, and also we have $\dim E = \dim E' = 1$. This makes it tempting to expect that in general $a = b = c_g$, and the CM abelian varieties representing the CM type (F, Φ) have dimension bounded by g (i.e. $\dim_K \Phi \leq g$). While we believe such a result should be true, we do not know how to prove it in general, even assuming GRH. However, we can prove a modified version of this statement under some additional assumptions; see Corollary 5.19. We also can improve our bound on $\dim_K \Phi$ and show that $\dim_K \Phi \leq g$ for $d = \deg \psi = 1$, using the following observation. If ψ_0 is an associated character of A , then $\text{cyc}_\ell^d \otimes \psi_0^{-1}$ is also an associated character of A , due to the Galois-invariance of the Weil pairing. Thus, to describe all of the associated

characters of A , it suffices to consider one character in each pair $\{\psi_0, \text{cyc}_\ell^d \otimes \psi_0^{-1}\}$. Now we state the main theorem of our paper.

Theorem 4 (Theorem 5.16). *Let K be a number field, and g and d be positive integers. Then, there exists a finite set $S_{K,g}$ of prime numbers depending only on K and g , and a constant $0 < c_g < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g -dimensional abelian variety A with a mod- ℓ associated character ψ_0 of degree d , we have*

$$\psi^{e \cdot w} \equiv \psi_{F,\Phi}^w \pmod{\ell},$$

where ψ is either ψ_0 or $\text{cyc}_\ell^d \otimes \psi_0^{-1}$ and $w = \frac{\text{lcm}(N, c_g)}{\text{gcd}(e, c_g)}$. Here, F is either \mathbb{Q} or a CM-field, and $\Phi: F \rightarrow \text{End}(K^m)$ is a primitive balanced representation such that $K \supset K_{F,\Phi}$. The quantities a , e , and N are integers with e and N positive, which satisfy $m = \frac{1}{2} \cdot a \cdot e \cdot [F : \mathbb{Q}]$. Moreover, $0 \leq a \leq d$, and both $\varphi(N)$ and $e \cdot [F : \mathbb{Q}]$ are at most $\binom{2g}{d}$.

We think of Φ as giving the isomorphism class of the K - F bimodule $\text{Lie}(B)$, for any abelian variety B with CM type (F, Φ) . The above bounds imply that $m = \dim B \leq \frac{d}{2} \cdot \binom{2g}{d}$. In particular, if $d = 1$, then $m = \dim B \leq g = \dim A$.

The proof of Theorem 4 implies that the set $S_{K,g}$ is effectively computable. In Theorem 7.9, we give an explicit bound on the value of $\prod_{\ell \in S_{K,g}} \ell$.

The relationship between mod- ℓ and ℓ -adic characters becomes particularly nice when K has semistable reduction at all primes over ℓ and the associated character has degree 1 (i.e. is a one-dimensional subquotient). In this case, we get a very similar result to the conditional statement of Theorem 1.

Corollary 5 (Corollary 5.19). *Let K be a number field, and g and d be positive integers. Then, there exists a finite set $S_{K,g}$ of prime numbers depending only on K and g , and a constant $0 < c_g < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g -dimensional abelian variety A with a mod- ℓ associated character ψ of degree 1, one of the following holds.*

1. *The character ψ^{c_g} is trivial or equal to $\text{cyc}_\ell^{c_g}$.*
2. *There exists an abelian unramified extension M/K , a (full) CM abelian variety A' defined over M , such that K contains the reflex field of the CM field of A' (which in particular implies that A' has CM defined over M), and an ℓ -adic associated character of degree 1 of A' , whose mod- ℓ reduction ψ' satisfies*

$$(\psi|_{\text{Gal}(\overline{K}/M)})^{c_g} = (\psi')^{c_g} \quad \text{and} \quad (\dim A') \cdot (\text{exponent } M/K) \leq g.$$

When A is an abelian surface and $d = 1$, the result of Theorem 4 can be formulated more concisely.

Corollary 6 (Corollary 5.20). *Let K be a number field. Then there exists a finite set S_K of prime numbers depending only on K such that, for a prime $\ell \notin S_K$, and an abelian surface A with a mod- ℓ associated character ψ of degree 1, one of the following holds.*

1. *There exists a full CM abelian surface A' over K whose CM is defined over K , with an ℓ -adic degree 1 associated character whose mod- ℓ reduction ψ' satisfies*

$$\psi^{120} = (\psi')^{120}.$$

2. *There exists an abelian unramified extension L/K of exponent at most 2, a CM elliptic curve E' defined over L , such that K contains the CM field, and an ℓ -adic degree 1 associated character of E' whose mod- ℓ reduction ψ' satisfies*

$$\psi|_{\text{Gal}(\overline{K}/L)}^{120} = (\psi')^{120}.$$

3. *For some $a \in \{0, 60, 120\}$, we have*

$$\psi^{120} = \text{cyc}_\ell^a.$$

There is a similar formulation for abelian threefolds (see Corollary 5.21), but not for higher-dimensional abelian varieties; this corresponds to the fact that for $g \geq 4$, the relevant Shimura varieties may have nonzero dimension.

If $A = \text{Alb}(X)$ is the Albanese variety of a smooth proper scheme X of finite type over K , then we can apply Theorem 4 to A . For ℓ sufficiently large, Theorem 4 gives nontrivial restrictions on the action of G_K on the étale cohomology $H^1(X, \mathbb{F}_\ell) \simeq H^1(\text{Alb}(X), \mathbb{F}_\ell)$. We believe it may be possible to study the associated characters of the higher étale cohomology groups $H^r(X, \mathbb{F}_\ell)$ using our methods. Indeed, in several cases — e.g. when X has everywhere good reduction — our techniques give an analogous result for $H^r(X, \mathbb{F}_\ell)$. However, in the general case there are some difficulties that occur due to the lack of a good theory of semistable reduction for arbitrary smooth proper schemes (see Remark 5.1 for details).

Our proof of Theorem 4 is similar in spirit to the method used by Serre in [17] to classify elliptic curves with non-surjective mod- ℓ Galois action. Working with abelian varieties instead of elliptic curves introduces additional issues. This is because while there are only finitely many elliptic curves with a given endomorphism ring larger than \mathbb{Z} , there are families of abelian varieties with extra endomorphisms parameterized by positive-dimensional Shimura varieties. This forces the theory of associated characters to become more complicated, once these Shimura varieties enter into the picture. Moreover, obtaining uniform bounds requires a more delicate analysis than Serre's [17], in particular because we cannot assume that A is everywhere semistable by extending the ground field.

The paper consists of two main essentially independent parts. In the first part, we explicitly compute the ℓ -adic associated characters of abelian varieties in terms of class

field theory. This analysis is relatively simple, but requires a number of technical results including Faltings' Theorem [4] and the theory of Shimura varieties of PEL type [3]. It also uses the local characterization of determinants of subquotients of the p -adic Tate module, proved by Brian Conrad in Appendix A using p -adic Hodge theory. The second part of the paper, about mod- ℓ associated characters, is significantly more involved but uses less machinery. We use a result of Raynaud to get control over the action of the inertia groups at primes dividing ℓ , and use the Weil conjectures (and Grothendieck's generalization in [6] for primes of bad reduction) to control the behavior of Frobenius elements at primes not dividing ℓ . These pieces of information are then combined to produce a list of explicit expressions for the mod- ℓ associated characters in terms of class field theory. This list turns out to be remarkably similar to the list of ℓ -adic characters found in the first part of the paper (see Theorem 4).

We now describe the structure of the paper. In Section 2, we introduce the language of algebraic characters which we will use throughout the paper.

In Section 3 we study abelian varieties B with CM defined over K and their associated determinantal characters; we also compute the separating fields of some Shimura varieties classifying (F, Φ) abelian varieties.

Then we turn to studying mod- ℓ associated characters. We begin in Section 4 by studying the local behavior of these characters. In 4.1 and 4.2, we recall some facts about the action of Frobenius elements on the Tate module and about semistable reduction of abelian varieties respectively. In 4.3, we analyze the restriction of ψ to the inertia subgroups.

In Section 5, we study the global properties of these characters, using the results from Section 4. In particular, the analysis in Section 5 will apply to any Galois character that satisfies the key results from Section 4; for details see Remark 5.1. In 5.2, we prove several restrictions on the character ψ using its values on Frobenius elements. Subsection 5.3 is devoted to the proof of the Theorem 4, our main result. Finally, in 5.4, we derive some corollaries of the main theorem.

In Section 6, we apply the main theorem to elliptic curves and prove Theorem 1 and Corollary 6.5 about isogenies of elliptic curves.

Finally, in Section 7, we make all of our arguments effective, proving effective versions of the main theorem both for elliptic curves and abelian varieties (Theorems 7.2 and 7.9).

Notation Conventions: Throughout the paper, we normalize the Artin map to carry uniformizers to *arithmetic* Frobenius elements, i.e. the map $\alpha \mapsto \alpha^q$. We write n_K , r_K , R_K , h_K , and Δ_K for the degree, rank of the unit group, regulator, class number, and discriminant of K respectively.

Acknowledgements

We would like to thank David Zureick-Brown, Bryden Cais and Ken Ono for giving us the problem that led to this paper and answering questions. We are grateful to Brian

Conrad for writing Appendix A. Thanks also to Brian Conrad, Jordan Ellenberg, Benedict Gross, Mark Kisin, Barry Mazur, Jean-Pierre Serre and Vadim Vologodsky for valuable comments and discussions. Finally we would like to express our admiration for Serre's paper [17] whose techniques provide the mathematical inspiration and departure-point of our work.

2 Algebraic Characters

A multiplicative map of number fields of algebraic origin — for example the norm map $\text{Nm}: K^\times \rightarrow \mathbb{Q}^\times$ — can be thought of as the induced map on \mathbb{Q} -points of a map of commutative algebraic groups over \mathbb{Q} . Such maps — which we will call *algebraic characters* — will appear for us as determinants of representations induced by CM (in Section 3.1) and as Galois characters (see Definition 2.23). In this section, we will introduce two main ways of thinking about algebraic characters — a concrete description as products of embeddings (Proposition 2.3) and an equivalent picture as determinants of representations (Proposition 2.9).

The main technical result of this section, Lemma 2.24, will give a way of defining global *Galois* characters from algebraic characters between global fields — an idea originally due to Serre (in [16]) but done here from the slightly different vantage point of CM fields and groups of Weil numbers.

2.1 Definitions and first properties of algebraic characters

We will be interested in algebraic characters between pairs of global number fields and pairs of p -adic number fields, but will first give some general definitions over any base field Q . Suppose that K and L are algebraic extensions of a base field Q and K/Q is finite. Write T_K and T_L for the algebraic tori $\text{Res}_Q^K \mathbb{G}_{m,K}$ and $\text{Res}_Q^L \mathbb{G}_{m,L}$, viewed as algebraic groups over Q .

Definition 2.1. An *algebraic character* is a multiplicative map $\theta: K^\times \rightarrow L^\times$ given by the map on Q -points of a morphism of algebraic groups $T_K \rightarrow T_L$.

Now pick an embedding $L \hookrightarrow \overline{Q}$.

Definition 2.2. We write Γ_K for the set of embeddings $K \hookrightarrow \overline{Q}$.

Proposition 2.3. *The (discrete) abelian group of multiplicative maps $\text{Hom}(T_K, T_L)$ is the group of invariants $\mathbb{Z}[\Gamma_K]^{G_L}$, with induced map on Q -points*

$$\sum_{\sigma \in \Gamma_K} a_\sigma \sigma: x \mapsto \prod (x^\sigma)^{a_\sigma} \quad \text{for } x \in T_K(Q) = K^\times.$$

Proof. See [16], section 1.1 of chapter 2. □

Corollary 2.4. *If L contains the Galois closure $K^{gal} \subset \overline{Q}$ of K , then*

$$\text{Hom}(T_K, T_L) = \mathbb{Z}[\Gamma_K].$$

Remark 2.5. For the purposes of this paper, one can always think of algebraic characters as maps $K^\times \rightarrow L^\times$ of form given by Proposition 2.3.

Definition 2.6. For $S = \sum S(\sigma) \cdot \sigma \in \mathbb{Z}[\Gamma_K]$, we define the algebraic character θ^S via

$$\theta^S(x) = \prod \sigma(x)^{S(\sigma)}.$$

Definition 2.7. We say that a character $\theta: T_K \rightarrow T_L$ is *positive* if it extends from T_K to $\text{Res}_Q^K \mathbb{A}_K^1$, or equivalently if $\theta = \theta^S$ for $S = \sum S(\sigma) \cdot \sigma$ with all $S(\sigma)$ nonnegative. Similarly, we say that θ is *negative* if $\theta \circ (x \mapsto x^{-1})$ is positive.

Definition 2.8. We define the *degree* of an algebraic character θ^S to be $\max_{\sigma \in \Gamma_K} |S(\sigma)|$.

Now we give the dictionary between characters and representations. Suppose V is a $K \otimes_Q L$ bimodule which is finite-dimensional as an L -module. Thinking of V as an L -vector space with an action of the (algebraic) group K^\times , we define $\det_L V: K^\times \rightarrow L^\times$ via the L -determinant of the K -action, i.e.

$$a \mapsto \det_L ((x \mapsto a \cdot x): V \rightarrow V).$$

Proposition 2.9. *For any positive algebraic character $\theta: K^\times \rightarrow L^\times$, there is a $K \otimes_Q L$ -bimodule V which is finite-dimensional as an L -module and such that $\det_L V = \theta$. Moreover, the bimodule V is unique up to isomorphism.*

Proof. Suppose at first that $L = \overline{Q}$. Let the a_σ be as in Proposition 2.3. Then the representation $V = \bigoplus_{\sigma \in \Gamma_K} a_\sigma \sigma$ is the required bimodule. This bimodule is unique since $K \otimes_Q \overline{Q} \simeq \bigoplus_{\sigma \in \Gamma_K} \overline{Q}[\sigma]$, where $\overline{Q}[\sigma]$ is a one-dimensional vector space over \overline{Q} such that the K -action is given by σ composed with the \overline{Q} -action.

For the general case, we invoke the primitive element theorem to write $K = Q[\alpha]$; note that our representation is determined by the matrix for α up to conjugacy. The result thus follows from the following standard result of linear algebra applied to $N/M = \overline{Q}/L$, where the Galois-invariance is evident in the proof of the case $L = \overline{Q}$: Given a field extension N/M , the intersection of any Galois-invariant conjugacy class of $\text{GL}_n(N)$ with $\text{GL}_n(M)$ is a conjugacy class of $\text{GL}_n(M)$. (This last fact follows from the invariance of the rank of a matrix under base extension.) \square

Remark 2.10. When K and L are both finite-dimensional over Q , the above proposition gives a curious duality between algebraic characters $K^\times \rightarrow L^\times$ and $L^\times \rightarrow K^\times$, known as the reflex map.

Now suppose that $\mathcal{O} \subset Q$ is an integrally closed subring. Since embeddings of fields preserve rings of integers, Proposition 2.3 implies that any algebraic character $\theta: K^\times \rightarrow L^\times$ sends $\mathcal{O}_K^\times \subset K^\times$ to $\mathcal{O}_L^\times \subset L^\times$.

Definition 2.11. For an ideal $I \subset \mathcal{O}_L$ and algebraic character $\theta: K^\times \rightarrow L^\times$ we define

$$\theta \bmod I: \mathcal{O}_K^\times \rightarrow (\mathcal{O}_L/I)^\times$$

to be the map induced by composing with $\mathcal{O}_L^\times \rightarrow (\mathcal{O}_L/I)^\times$. We call a character of the above form a *reduction of an algebraic character*.

We will be particularly interested in the case where $Q = \mathbb{Q}_p$ and $I = m_L$ is the maximal ideal of \mathcal{O}_L , giving a map $\theta \bmod m_L: \mathcal{O}_K^\times \rightarrow k_L^\times$.

2.2 ℓ -adic characters induced from global characters

Suppose K/\mathbb{Q} is a number field and ℓ is a prime. We will take $L = \overline{\mathbb{Q}}$, and fix an embedding $\iota: \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$.

Proposition 2.12. *There is a (unique) bijective correspondence*

$$(\theta \mapsto \theta_\ell): \text{Hom}(T_K, T_{\overline{\mathbb{Q}}}) \xrightarrow{\sim} \text{Hom}\left(\prod_{v|\ell} T_{K_v}, T_{\overline{\mathbb{Q}}_\ell}\right),$$

with the property that the maps on points $K^\times \rightarrow \overline{\mathbb{Q}}^\times$ and $\prod K_v^\times \rightarrow \overline{\mathbb{Q}}_p^\times$ fit into the commutative diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{\theta} & \overline{\mathbb{Q}} \\ \downarrow & & \downarrow \iota \\ \prod_{v|\ell} K_v & \xrightarrow{\theta_\ell} & \overline{\mathbb{Q}}_\ell \end{array}$$

Definition 2.13. We will call this bijective correspondence *localization* of characters.

Proof. Note that if θ_ℓ exists, it is unique since $K^\times \subset \prod_{v|\ell} K_v$ is dense. Now suppose $\theta = \sigma$ is a single embedding. Then by the decomposition theorem for ideals under of finite extensions, the composition $\iota \circ \sigma$ can be uniquely written as $K \subset K_v \xrightarrow{\sigma_\ell} \overline{\mathbb{Q}}_\ell$, where $\sigma_\ell \in \Gamma_{K_v}$. Having constructed σ_ℓ for $\sigma \in \Gamma_{K_v}$ which fits into the diagram in the proposition, we define θ_ℓ for arbitrary θ multiplicatively. This is an isomorphism $\text{Hom}(T_K, T_{\overline{\mathbb{Q}}}) \xrightarrow{\sim} \text{Hom}(\prod_{v|p} T_{K_v}, T_{\overline{\mathbb{Q}}_\ell})$ as it induces a bijection between generators of two free groups. \square

2.3 Galois characters induced from algebraic characters

Localizing an algebraic character $\theta: K^\times \rightarrow L^\times$ of global fields, one can define a number of characters on the group of idèles (for example, by considering the induced map on adelic points $T_K(\mathbb{A}) \rightarrow T_L(\mathbb{A})$), which will in some cases descend to Galois characters. Here we give such a construction in a rather specific case, which will be of interest in the rest of the paper.

Definition 2.14. We say that an algebraic character $\theta: K^\times \rightarrow L^\times$ is *balanced* if the product $\theta \cdot (\theta \circ \sigma)$ is a power of $\text{Nm}_{\mathbb{Q}}^K$ for *any* complex conjugation $\sigma \in \text{Gal}(L/\mathbb{Q})$. Otherwise, we say θ is *unbalanced*. Similarly, we say an K - L bimodule V is balanced (resp. unbalanced) if the character $\det_L V$ is balanced (resp. unbalanced).

The following two lemmas, which will play a central role in the following sections, show that if we hope to extend an algebraic character θ (thought of as a Galois character of a product of local field) to a *global* Galois group, then (under certain mild ramification conditions) θ has to be balanced.

Lemma 2.15. *The character θ^S is balanced if and only if $\theta^S(u)$ is a root of unity for any unit $u \in \mathcal{O}_K^\times$.*

Proof. Let us order the σ_i so that $\sigma_1, \sigma_2, \dots, \sigma_{r_1}$ are real embeddings, and σ_{r_1+i} is the complex conjugate of $\sigma_{r_1+r_2+i}$. Consider the multiplicative Minkowski embedding, i.e. the map $\mu: \mathcal{O}_K^\times \rightarrow \mathbb{R}^{r_K+1}$ given by

$$\mu: x \mapsto (\log |\sigma_1(x)|, \log |\sigma_2(x)|, \dots, \log |\sigma_{r_1}(x)|, 2 \log |\sigma_{r_1+1}(x)|, \dots, 2 \log |\sigma_{r_1+r_2}(x)|).$$

Dirichlet's unit Theorem states that the kernel of μ is roots of unity and the image of μ is a lattice in $\mathbb{R}^{r_K+1}_0$, the subspace of vectors in \mathbb{R}^{r_K+1} whose sum of coordinates is zero. Call this lattice $\Lambda = \text{Im}(\mu) \subset \mathbb{R}^{r_K+1}_0$. Observe that for any $S \in \mathbb{Z}[\Gamma_K]$, the function

$$(x \mapsto \log |\theta^S(x)|) = f^S \circ \mu$$

factors as the composition of μ with a linear function $f^S: \mathbb{R}^{r_K+1} \rightarrow \mathbb{R}$. Since $\theta^S(u)$ is a root of unity for any unit $u \in \mathcal{O}_K^\times$, it follows that f^S vanishes on units; moreover, since f^S is linear, f^S vanishes on the hyperplane spanned by the units. Hence it must be a multiple of the defining equation of the hyperplane, $\sum_{i=1}^{r_1+r_2} x_i$.

The converse follows from the fact that if $|\theta(u)| = 1$ under any complex embedding, then $\theta(u)$ is a root of unity. \square

Lemma 2.16. *If the localization θ_ℓ^S coincides on an open subgroup $U \subset \prod_{v|\ell} \mathcal{O}_{K_v}^\times$ with the composition*

$$\prod_{v|\ell} \mathcal{O}_{K_v}^\times \longrightarrow \mathbb{I}_K \longrightarrow \text{Gal}(K^{ab}/K) \xrightarrow{\psi} \overline{\mathbb{Q}}_\ell^\times$$

for a character $\psi: \text{Gal}(K^{ab}/K) \rightarrow \overline{\mathbb{Q}}_\ell^\times$ which is ramified at only finitely many primes and has finite ramification index at primes not lying over ℓ , then θ^S is balanced.

Proof. Let $(\mathcal{O}_K^\times)_\ell$ be the image of the group of units under the embedding $\mathcal{O}_K^\times \hookrightarrow \prod_{v|\ell} \mathcal{O}_{K_v}^\times$, and let $U_\ell \subset \mathbb{I}_K$ be the subgroup $(\mathcal{O}_K^\times)_\ell \times \prod_{v \nmid \ell} \mathcal{O}_{K_v}^\times$. Then the image of U_ℓ in \mathbb{I}_K/K^\times coincides with the image of $\prod_{v \nmid \ell} \mathcal{O}_{K_v}^\times$, which (by the finite ramification outside of ℓ assumption) has finite image under ψ . On the other hand, $\psi(U_\ell)$ contains a subgroup of finite index of the image $\theta^S(\mathcal{O}_K^\times)$. Hence, the image of \mathcal{O}_K^\times under θ^S is finite, so θ^S is balanced by Lemma 2.15. \square

Next we prove a converse — that if the character *is* balanced then we can in fact extend it to a global Galois character with appropriately mild ramification behavior.

Definition 2.17. The *group of Weil elements* $W_L \subset L^\times$ is the group of elements $w \in L^\times$ satisfying $w \cdot \sigma(w) \in \mathbb{Q}^\times$ for *any* complex conjugation $\sigma \in \text{Gal}(K^{\text{gal}}/\mathbb{Q})$.

Definition 2.18. We say that F is a *CM field* if *any* complex conjugation restricts to the same nontrivial element of $\text{Gal}(F^{\text{gal}}/\mathbb{Q})$. Equivalently, F is a CM field if F is a quadratic totally imaginary extension of a totally real subfield.

It is easy to see that a balanced character $K^\times \rightarrow L^\times$ factors through an embedding $F \subset L$, where F is either a CM field or $F = \mathbb{Q}$. We will from now on take F to be a CM field (or \mathbb{Q}) and $\theta: K \rightarrow F$ to be an algebraic character.

Definition 2.19. The *Weil class group* $\text{Cl}^W(F) = I_F/W_F$ is the group of fractional ideals modulo the group of Weil elements of F . (Note that it is in general an infinite group.)

As θ is a map of algebraic groups, θ induces a map from the idèles of K to the idèles of L . Since θ is balanced, the image (viewed as a map $K^\times \rightarrow F^\times$) of θ lies in the group of Weil elements of F .

Definition 2.20. We define $C\theta: \text{Cl}(K) \rightarrow \text{Cl}^W(F)$ to be the map induced by θ .

Definition 2.21. Write \mathbb{I}_K^θ for the group of idèles of K whose ideal class is in the kernel of $C\theta$. Write K_θ for the abelian extension of K corresponding to the subgroup $\mathbb{I}_K^\theta \subset \mathbb{I}_K$.

Definition 2.22. We write N_0 for the number of roots of unity in F , and $\mu_F = \mu_{N_0}$ for the group of roots of unity in F .

A Weil element which is a unit has norm 1 under any complex embedding, and hence is a root of unity. Therefore, θ induces a map $I\theta$ from \mathbb{I}_θ to W_F/μ_F . Now, we fix an embedding $F \hookrightarrow \overline{\mathbb{Q}_\ell}$.

Definition 2.23. For a map $\theta: K^\times \rightarrow F^\times \subset \overline{\mathbb{Q}^\times}$, we define the character $\psi_\theta: \mathbb{I}_K^\theta \rightarrow \overline{\mathbb{Q}_\ell}/\mu_F$ via $\psi_\theta := I\theta \cdot \theta_\ell^{-1}$.

Slightly abusing notation, given a $K - F$ bimodule Φ we define $\psi_{F,\Phi} := \psi_\theta$ for $\theta = \det_K \Phi: K^\times \rightarrow \overline{\mathbb{Q}^\times}$.

Lemma 2.24. *The character ψ_θ is trivial on principal idèles and has image contained in $\mathcal{O}_{\mathbb{Q}_\ell}^\times / \mu_F$.*

Proof. To show triviality on principal idèles, it suffices to note that given $x \in K^\times$, we have an equality of principal ideals $(I\theta(x)) = (\theta(x))$, both of which are generated by a Weil number. To show that the image lies in $\mathcal{O}_{\mathbb{Q}_\ell}^\times$, it suffices to note that $\psi_\theta(\pi_v)$ and $\theta_\ell(\pi_v)$ have the same norm for $\pi_v \in K_v$ a uniformizer. \square

Extending the character to infinite places by the trivial map, this lets us define a Galois character (on $\text{Gal}(\overline{K}/K_\theta)$) given any CM field F and balanced character $K^\times \rightarrow F^\times$.

Remark 2.25. The above character is uniquely determined by the property that it takes any uniformizer π_w for $w \nmid \ell$ and with $[w] \in \ker C\theta$ to a Weil number generating the ideal $I\theta(w)$ (up to roots of unity).

3 Abelian Varieties with Complex Multiplication

3.1 Galois Characters Associated to CM Abelian Varieties

Let B be an abelian variety defined over a field K of characteristic zero. Recall that we say B has endomorphisms by a number field E if there is an injection $\iota: E \hookrightarrow \text{End}_K(B) \otimes \mathbb{Q}$.

The p -adic Tate module is a finite-dimensional $(E \otimes \mathbb{Q}_p)$ -module, so we can take the determinant over $(E \otimes \mathbb{Q}_p)$ of the Galois action. (If we write $E \otimes \mathbb{Q}_p = \prod_{v|p} E_v$, this is just the product of the E_v -linear determinants.) This determinant of the Galois action gives us a map $\text{Gal}(\overline{K}/K) \rightarrow (E \otimes \mathbb{Q}_p)^\times$.

Note that the E -action gives a decomposition of the Tate module with extended coefficients, $B[p^\infty] \otimes \overline{\mathbb{Q}_p}$, into eigenspaces (corresponding to embeddings $E \hookrightarrow \overline{\mathbb{Q}_p}$). The $E \otimes \mathbb{Q}_p$ -determinant encodes the $\overline{\mathbb{Q}_p}$ -determinants (i.e. associated characters) of each of these eigenspaces. The $\overline{\mathbb{Q}_p}$ -determinant of the σ -eigenspace of E is given by the character $\psi_{B,\sigma}$ defined as follows.

Definition 3.1. Define the character

$$\psi_{B,\sigma} := (\sigma \otimes \text{id}) \circ \det_{E \otimes \overline{\mathbb{Q}_p}} B[p^\infty] \otimes \overline{\mathbb{Q}_p}.$$

We will see that the study of ℓ -adic associated characters can be reduced to studying the characters $\psi_{B,\sigma}$. Namely, suppose that B is an abelian variety. Let V and W be subspaces of $B[\ell^\infty] \otimes \overline{\mathbb{Q}_\ell}$; write V^0 and W^0 for $V \cap B[\ell^\infty] \otimes \overline{\mathbb{Z}_\ell}$ and $W \cap B[\ell^\infty] \otimes \overline{\mathbb{Z}_\ell}$ respectively. We define the distance function $d(V, W) = \ell^{-n(V,W)}$, where

$$n(V, W) = \max \{ m : V^0 + \ell^m B[\ell^\infty] \otimes \overline{\mathbb{Z}_\ell} = W^0 + \ell^m B[\ell^\infty] \otimes \overline{\mathbb{Z}_\ell} \}.$$

Then we have the following lemma.

Lemma 3.2. *Suppose B is an abelian variety over a number field K . Let V be an irreducible G_K -equivariant subspace (or, in this case equivalently, subquotient) of $B[\ell^\infty] \otimes \overline{\mathbb{Q}_\ell}$. Then for any $\epsilon > 0$, there is an $\alpha \in \text{End}(B)$ such that $d(V, W) \leq \epsilon$ for some eigenspace W of the action of α on $B[\ell^\infty] \otimes \overline{\mathbb{Q}_\ell}$.*

Proof. Let $V = \sigma_0 V, \sigma_1 V, \dots, \sigma_m V$ be the conjugates of V under the action of $\text{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$. By a theorem of Faltings (Theorem 3 of [4]), the Galois representation $B[\ell^\infty] \otimes \mathbb{Q}_\ell$ is semisimple. This means it remains semisimple after extending coefficients to $\overline{\mathbb{Q}_\ell}$, and so $B[\ell^\infty] \otimes \overline{\mathbb{Q}_\ell} = \sigma_0 V \oplus \dots \oplus \sigma_m V \oplus V'$ for some subrepresentation V' . Now let H be the subgroup of $G_{\mathbb{Q}_\ell}$ of elements which take V to itself, and let $\mathcal{K} \subset \overline{\mathbb{Q}_\ell}$ be the fixed subfield of H . The extension $\mathcal{K}/\mathbb{Q}_\ell$ is finite, so we can choose $\alpha \in \mathcal{K}$ a primitive element over \mathbb{Q}_ℓ . Now we define an endomorphism

$$\alpha_0 = \sigma_0(\alpha) \cdot \text{id}_{\sigma_0 V} \oplus \dots \oplus \sigma_m(\alpha) \cdot \text{id}_{\sigma_m V} \oplus 0_{V'} : B[\ell^\infty] \otimes \overline{\mathbb{Q}_\ell} \rightarrow B[\ell^\infty] \otimes \overline{\mathbb{Q}_\ell},$$

and notice that it is $\text{Gal}(\mathcal{K}/\mathbb{Q}_\ell)$ -invariant, and hence α_0 restricts to a G_K -invariant endomorphism $\alpha_0 : B[\ell^\infty] \otimes \mathbb{Q}_\ell \rightarrow B[\ell^\infty] \otimes \mathbb{Q}_\ell$.

Another theorem of Faltings (Theorem 4 of [4]) gives that

$$\text{End}(B) \otimes \mathbb{Q}_\ell \cong \text{End}_{G_K}(B[\ell^\infty] \otimes \mathbb{Q}_\ell).$$

In particular, there is an element $\alpha \in \text{End } B \otimes \mathbb{Q}$ whose induced map on the Tate module approximates α_0 to arbitrary ℓ -adic precision. Then V is arbitrarily close to a single eigenspace of the action of α on $B[\ell^\infty] \otimes \overline{\mathbb{Q}_\ell}$. \square

Now suppose B is simple (we can study the general case by decomposing B up to isogeny into a product of simple abelian varieties). We take $E = \mathbb{Q}(\alpha)$, so $\det_W = \psi_{B, \sigma}$. In the next two sections, we will see that up to multiplication by roots of unity in E , the character $\psi_{B, \sigma}$ is determined by the field E plus some *finite* combinatorial data. In particular (up to multiplication by bounded roots of unity), there are only finitely many characters giving the Galois action \det_W in the above lemma; it follows by taking a sufficiently good approximation W that one of these finitely many characters gives the action on \det_V .

3.2 Local Case

Suppose that $K = \mathcal{K}$ is a p -adic field. By local class field theory, we have a natural map $\text{rec} : \mathcal{K}^\times \rightarrow \text{Gal}(\mathcal{K}^{\text{ab}}/\mathcal{K})$.

Now, consider the determinant of the Galois action $\text{Gal}(\overline{\mathcal{K}}/\mathcal{K}) \rightarrow (E \otimes \mathbb{Q}_p)^\times$. Since $(E \otimes \mathbb{Q}_p)^\times$ is an abelian group, this map factors through $\text{Gal}(\mathcal{K}^{\text{ab}}/\mathcal{K})$. Precomposing with the reciprocity homomorphism, we get a map $\mathcal{K}^\times \rightarrow (E \otimes \mathbb{Q}_p)^\times$. Write $\text{Lie}(B)$ for the tangent space to the identity element of B . Since $\mathbb{Q}_p \subset \mathcal{K}$ acts on $\text{Lie}(B)$, the Lie algebra $\text{Lie}(B)$ naturally has the structure of an $(E \otimes \mathbb{Q}_p)$ - \mathcal{K} bimodule. We get another map $\mathcal{K}^\times \rightarrow (E \otimes \mathbb{Q}_p)^\times$ induced by taking the determinant over $E \otimes \mathbb{Q}_p$ of the \mathcal{K}^\times -action

on the $(E \otimes \mathbb{Q}_p)\text{-}\mathcal{K}$ bimodule $\text{Lie}(B)$ (c.f. Proposition 2.9). These maps do not necessarily coincide, but they almost do (up to sign); namely, we have the following theorem, due to Conrad.

Theorem (Conrad, Appendix A). *Let B be an abelian variety defined over a local field \mathcal{K} of residue characteristic p , which admits an injection $\iota: E \hookrightarrow \text{End}_{\mathcal{K}}(B) \otimes \mathbb{Q}$. Then, there is an open subgroup $U \subset \mathcal{O}_{\mathcal{K}}^{\times}$ on which the following diagram commutes.*

$$\begin{array}{ccc} U \subset \mathcal{K}^{\times} & \xrightarrow{\text{rec}} & \text{Gal}(\mathcal{K}^{ab}/\mathcal{K}) \\ \downarrow u \mapsto (x \mapsto u^{-1} \cdot x) & & \downarrow \det_{E \otimes \mathbb{Q}_p} \circ \rho_{B,p}^{\infty} \\ \text{Aut}_{E \otimes \mathbb{Q}_p}(\text{Lie}(B)) & \xrightarrow{\det_{E \otimes \mathbb{Q}_p}} & (E \otimes \mathbb{Q}_p)^{\times} \end{array}$$

Remark 3.3. When B has semistable reduction, we can take $U = \mathcal{O}_{\mathcal{K}}^{\times}$ (see Appendix A). By Lemma 4.6, this implies that we can take U to have index dividing the constant c_g defined in Section 4.2 below.

The above lemma implies that, choosing an embedding $\sigma: E \hookrightarrow \overline{\mathbb{Q}}_p$, the character $\psi_{B,\sigma}$ (Definition 3.1) is the same as $(\det_E \text{Lie}(B))_p$ (see Propositions 2.9 and 2.12) when restricted to an open subgroup.

3.3 Global Case

Now suppose K is a global field and B is a simple abelian variety over K . As explained in Section 3.1, any ℓ -adic associated character of B is given by a $\psi_{B,\sigma}$, corresponding to an eigenspace for the action of a number field $E \hookrightarrow \text{End}(B) \otimes \mathbb{Q}$. We see from Conrad's Theorem 3.2 above that $\psi_{B,\sigma}$ equals $(\det_E \text{Lie}(B))_{\ell}$ (in the notation of Definition 2.13), when restricted to an open subgroup of $\prod_{v|\ell} \mathcal{O}_v^{\times} \subset \text{Gal}(\overline{K}/K)^{ab}$.

Define $F \subset E$ to be the composite of all CM subfields of E (so F is either a CM field or $F = \mathbb{Q}$). Then we have the following lemma.

Lemma 3.4. *The E -representation $\text{Lie}(B)$ is induced from some F -representation Φ , i.e. $\text{Lie}(B) \simeq \Phi \otimes_F E$. Moreover, $\det_E \text{Lie}(B) = \det_F \Phi$.*

Proof. By Lemma 2.16, $\det_E \text{Lie}(B)$ is a balanced character, and hence has image contained in a CM field (or \mathbb{Q}). Equivalently by Lemma 2.9, the E -module $\text{Lie}(B)$ is induced from a module over F , i.e. $\text{Lie}(B) \simeq \Phi \otimes_F E$ for some F - K bimodule Φ . It follows that $\det_E \text{Lie}(B) = \det_F \Phi$. \square

Definition 3.5. We say that a polarized abelian variety B is a (F, Φ) -abelian variety if B has endomorphisms by a number field $E \supset F$ such that the action of E makes $\text{Lie}(B) \simeq \Phi \otimes_F E$ as an E - K bimodule. We call (F, Φ) the *CM-type* of B .

Lemma 3.4 shows that any ℓ -adic associated character of a simple abelian variety is a product of characters of the form $\psi_{B,\sigma}$ for an (F, Φ) -abelian variety B .

Theorem 3.6. *Suppose B is an (F, Φ) abelian variety and $\theta : K \rightarrow \overline{\mathbb{Q}}$ is the algebraic character $\det_F \Phi$ induced from Φ under the correspondence of Proposition 2.9. Then, in the notation of Definitions 2.21 and 2.23 we have $K = K_\theta$ and $\psi_{B,\sigma} \equiv \psi_\theta \pmod{\mu_F}$.*

Before proving the theorem, we give an equivalent statement which we will use in the following sections. Let $\theta = \det_F \Phi$ as before, and write $F' \subset K$ for the minimal field such that $\theta : K^\times \rightarrow F'^\times$ factors as the composition of $\text{Nm}_{F'}^K$ with $\theta_0 : F' \rightarrow F$.

Definition 3.7. We write $K_{F,\Phi} = K_{\theta_0}$ and $\psi_{F,\Phi} = \psi_{\theta_0}$.

Remark 3.8. We have $K_\theta = K \cdot K_{F,\Phi}$, and $\psi_\theta = \psi_{\theta_0} \circ \text{Nm}_{F'}^K$. Both the field $K_{F,\Phi}$ and the character $\psi_{F,\Phi}$ are *geometric* invariants of B ; i.e. they are unchanged under base extensions.

Unwinding the definitions, we see that the first part of Theorem 3.6 is equivalent to the assertion that $K \supset K_{F,\Phi}$.

Proof of Theorem 3.6. First we show that $\psi_{B,\sigma} \equiv \psi_\theta \pmod{\mu_F}$ restricted to $\text{Gal}(\overline{K}/K_\theta)$, where both characters are defined. Consider the quotient

$$\epsilon := \psi_{B,\sigma}/\psi_\theta : \text{Gal}(\overline{K}/K_\theta) \rightarrow \overline{\mathbb{Q}}_\ell/\mu_F.$$

The two characters $\psi_{B,\sigma}$ and ψ_θ coincide on an open subgroup of any inertia subgroup $\mathcal{O}_{K_v}^\times \subset \mathbb{I}_K$ for $v \mid \ell$ and have finite ramification degree outside of ℓ , so the image of ϵ is finite. Now, we use the following lemma.

Lemma 3.9. *For any prime v of good reduction for B , there is an embedding $E \subset \overline{\mathbb{Q}}_\ell$ such that $\psi_{B,\sigma}(\pi_v) \in E \subset \overline{\mathbb{Q}}_\ell$. Furthermore, if $F \neq \mathbb{Q}$, then $\psi_{B,\sigma}(\pi_v) \in F^\times$.*

Proof. We have $\psi_{B,\sigma}(\pi_v) \in E \subset \overline{\mathbb{Q}}_\ell$ by paragraph 11.10 of [19]. If $F \neq \mathbb{Q}$, then F contains all totally real fields as well as all CM fields; since $\psi_{B,\sigma}$ is a Weil number, it follows that $\psi_{B,\sigma} \in F$. \square

By definition, ψ_θ takes values in F^\times/μ_F , so ϵ takes Frobenius elements to elements of $\mu_E/\mu_F = \{1\}$. Hence, by the Chebotarev density theorem, ϵ is trivial.

Now it remains to prove that $K = K_\theta$. Although this follows from Lemma 3.11 of the next section, we give an alternative proof here. For $F = \mathbb{Q}$, this is immediate; thus, we assume $F \neq \mathbb{Q}$. Now suppose v is a prime ideal of K of good reduction for B . Since $\pi_v^{h_K} \in \text{Gal}(\overline{K}/K_\theta)$, we have $\psi_{B,\sigma}(\pi_v^{h_K}) \equiv \psi_\theta(\pi_v^{h_K}) \pmod{\mu_F}$. By Lemma 3.9, $\psi_{B,\sigma}(\pi_v) \in F$, so $(\psi_{B,\sigma}(\pi_v))^{h_K} = (\psi_\theta(\pi_v))^{h_K}$ as ideals of F . As the group of ideals of F is torsion-free, $(\psi_{B,\sigma}(\pi_v)) = (\psi_\theta(\pi_v))$. Hence, $\theta(v)$ is generated by $\psi_{B,\sigma}(\pi_v)$, which is a Weil element of F . By the Chebotarev density theorem, we conclude that $C\theta : \text{Cl}(K) \rightarrow \text{Cl}^W(F)$ is trivial, i.e. $K = K_\theta$. \square

3.4 Shimura Varieties and the Field $K_{F,\Phi}$

We have seen in the previous section that if there is an (F, Φ) -abelian variety B defined over a number field K , then K contains a certain field $K_{F,\Phi}$ associated to the CM type (F, Φ) . One can ask whether the converse holds, namely:

Question 1. Does there exist an abelian variety with CM by (F, Φ) defined (and with CM defined) over $K_{F,\Phi}$?

To the best of our knowledge, the above question is open, although we suspect it is false in general. However we give a statement (Theorem 3.11 below) which is the best we can do short of answering Question 1. This section will be devoted to formulating and proving this statement, which will boil down to a computation with Shimura varieties. No result from this section will be used in the rest of the paper.

Suppose X is a reduced scheme of finite type over a field $K \subset \mathbb{C}$ and $B \rightarrow X$ is a (flat) family of polarized abelian varieties over X .

Definition 3.10. The family $B \rightarrow X$ is a *strong (F, Φ) -family of abelian varieties* if there is a map of rings $\iota: \mathcal{O}_F \hookrightarrow \text{End}(B/X)$ making every \mathbb{C} -fiber of $B \rightarrow X$ an (F, Φ) -abelian variety with $E = F$ and $\theta \circ \iota(\overline{\alpha}) = \iota(\alpha)^* \circ \theta$, where $\theta: B \rightarrow B^\vee$ is the polarization.

We might hope to weaken Question 1 by replacing $\text{Spec } K_{F,\Phi}$ with a geometrically irreducible K -scheme X of finite type. In other words at least morally, for any field K , there should be a strong (F, Φ) -family of abelian varieties $B \rightarrow X$ over a geometrically irreducible K -scheme of finite type if and only if $K \supset K_{F,\Phi}$. The main result of this section will be the following theorem, which essentially states this is true if we allow “families whose members are defined up to isomorphism.” More precisely, we have:

Theorem 3.11. *Let (F, Φ) be a CM type, with Φ balanced. Then there exists a coarse moduli space of strong (F, Φ) -abelian varieties, which is defined over K provided that Φ is defined over K . Moreover, the separating field of this moduli space (i.e. the minimal field over which any irreducible component is geometrically irreducible) is $K_{F,\Phi}$.*

To prove this theorem, we will use the language of Shimura varieties classifying polarized abelian varieties with CM.

First we prove that Φ must be a balanced character, which can be reformulated as the following lemma.

Lemma 3.12. *There exists an (F, Φ) -abelian variety if and only if $\Phi \oplus \overline{\Phi} \simeq F^b \otimes_{\mathbb{Q}} K$ for some integer b (i.e. if and only if Φ is balanced).*

Proof. Suppose there was some (F, Φ) -abelian variety B defined over \mathbb{C} . Write $B(\mathbb{C}) = \mathbb{C}^g/\Lambda$. Note that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ is an F -vector space, hence isomorphic to F^b for some integer b . Therefore, as representations of F :

$$\Phi \oplus \overline{\Phi} \simeq \text{Lie}(B) \oplus \text{Lie}(B^\vee) \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{C} \simeq (\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \simeq F^b \otimes_{\mathbb{Q}} \mathbb{C}.$$

Now, we show the converse. Since $\Phi \oplus \overline{\Phi} \simeq F^b \otimes_{\mathbb{Q}} \mathbb{C}$ and all irreducible complex representations of F are one-dimensional, we can write

$$\Phi = \bigoplus_{i=1}^b \Phi_i \quad \text{where} \quad \Phi_i \oplus \overline{\Phi_i} \simeq F \otimes_{\mathbb{Q}} \mathbb{C}.$$

By the theory of complex multiplication [12], there exists a complex abelian variety B_i having CM by \mathcal{O}_F with CM type Φ_i . Then $B = \prod_{i=1}^b B_i$ is an (F, Φ) -abelian variety, completing the proof. \square

We now define and study the (coarse) moduli space of strong (F, Φ) -abelian varieties. This moduli space has infinitely many connected components, which we can remedy by keeping track of certain combinatorial data. The first such piece of data is the skew form $\langle \cdot, \cdot \rangle$ on the adelic Tate module $H_1(B, \widehat{\mathbb{Z}}) = \prod_{\ell} B[\ell^{\infty}]$ induced by the polarization. We can also keep track of the action $\alpha: \mathcal{O}_F \rightarrow \text{End}(H_1(B, \widehat{\mathbb{Z}}))$, which must satisfy

$$\langle \alpha(a) \cdot x, y \rangle = \langle x, \alpha(\overline{a}) \cdot y \rangle \quad \text{for all } a \in \mathcal{O}_F. \quad (3)$$

Furthermore, we note that as symplectic F -representations, $H_1(B, \widehat{\mathbb{Z}}) \simeq H_1(B, \mathbb{Z}) \otimes \widehat{\mathbb{Z}}$ and $\Phi \oplus \overline{\Phi} \simeq H_1(B, \mathbb{Z}) \otimes \mathbb{C}$, where $H_1(B, \mathbb{Z})$ is the singular homology of B with integral coefficients.

Definition 3.13. A *CM datum* is a quintuple $(F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$ where (F, Φ) is a CM type with Φ of dimension g over \mathbb{C} , Λ is a $2g$ -dimensional $\widehat{\mathbb{Z}}$ -lattice, $\langle \cdot, \cdot \rangle$ is a skew-symmetric integral form on Λ , and $\alpha: \mathcal{O}_F \rightarrow \text{End}(\Lambda)$ is an action of \mathcal{O}_F on Λ , satisfying formula (3). We additionally require that Λ is compatible with Φ : i.e., for some (not necessarily unique) \mathbb{Z} -lattice Λ_0 , we have $\Lambda_0 \otimes \widehat{\mathbb{Z}} \simeq \Lambda$ and $\Lambda_0 \otimes \mathbb{C} \simeq \Phi \oplus \overline{\Phi}$ as symplectic \mathcal{O}_F -modules.

We say that a polarized abelian variety B has CM datum $(F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$ if there is an isomorphism $H_1(B, \widehat{\mathbb{Z}}) \cong \Lambda$ with \mathcal{O}_F -action and polarization form induced by α and $\langle \cdot, \cdot \rangle$ respectively. We will often denote the CM datum by a single letter, $D = (F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$.

More generally, suppose X is a reduced scheme over K and that $B \rightarrow X$ is a strong (F, Φ) -family of abelian varieties. We say this family has CM datum $(F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$ if the \mathcal{O}_F -action induces CM datum $(F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$ on each \mathbb{C} -fiber. (A definition over arbitrary base schemes is possible but more involved; this one suffices for our purposes.)

One can ask whether the functor of families of (F, Φ) -abelian varieties with CM datum $D = (F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$ is representable. In general, it is not representable as a scheme, but is so as a (Deligne-Mumford) stack. We will consider here for simplicity the *coarse* moduli space S_D of such abelian varieties — the initial scheme which admits a map from this moduli stack (or via the Yoneda embedding, the initial scheme S such that $\text{Hom}(-, S)$ admits a map from the functor CM_D which assigns to a scheme the set of families over it with CM by D). Points of the coarse moduli space correspond canonically to (F, Φ) -abelian varieties with CM datum D up to isomorphism.

Let (F, Φ) be a CM type defined over a field K , and from now on suppose that the moduli space of strong (F, Φ) -abelian varieties is nonempty. Equivalently (by Lemma 3.12), suppose that $\Phi \oplus \overline{\Phi} \simeq F^b \otimes_{\mathbb{Q}} K$ for some integer b . Note that the moduli space of strong (F, Φ) -abelian varieties is a disjoint union over all possible sets of CM data D of the moduli space of strong (F, Φ) -abelian varieties with CM datum D . In order to prove Theorem 3.11 we will identify this latter moduli space with a Shimura variety (defined below).

Definition 3.14. If G is an algebraic group over k , and K is an extension of k , we define

$$G/K = G \times_{\mathrm{Spec} k} \mathrm{Spec} K.$$

Definition 3.15. We write $\mathbb{S} = \mathrm{Res}_{\mathbb{R}}^{\mathbb{C}} \mathbb{G}_{m, \mathbb{C}}$.

Definition 3.16. Let G be an algebraic group over the rationals, $h: \mathbb{S} \rightarrow G_{\mathbb{R}}$ be a map of real algebraic groups, and $G_{\mathcal{O}} \subset G(\mathbb{A}^f)$ be a compact subgroup. Writing K_{∞} for the stabilizer of h in $G(\mathbb{R})$, we define the *Shimura variety* to be the double coset space

$$\mathrm{Sh}_{G_{\mathcal{O}}}(G, h) := K_{\infty} \times G_{\mathcal{O}} \backslash G(\mathbb{A}) / G(\mathbb{Q}).$$

We will be interested in a particular class of Shimura varieties, corresponding to particular triples $(G, h, G_{\mathcal{O}})$ which we now describe. Let $D = (F, \Phi, \langle \cdot, \cdot \rangle, \alpha, \Lambda)$ be a CM datum, and Λ_0 be a \mathbb{Z} -lattice with $\Lambda_0 \otimes \widehat{\mathbb{Z}} \cong \Lambda$ and $\Lambda_0 \otimes \mathbb{C} \simeq \Phi \oplus \overline{\Phi}$ as symplectic \mathcal{O}_F -modules. While Λ_0 is noncanonical, $V = \Lambda_0 \otimes \mathbb{Q}$ (which we think of as a vector space over F) is uniquely determined by D by the Hasse-Minkowski principle for quadratic forms.

Definition 3.17. Define $\mathrm{GSp}(V)$ to be the group of F -linear maps $V \rightarrow V$ preserving $\langle \cdot, \cdot \rangle$ up to a (rational) scalar. We think of this as an algebraic group over \mathbb{Q} .

Take $G = \mathrm{GSp}(V)$, and let $G_{\mathcal{O}} \simeq G(\mathcal{O}_{\mathbb{A}^f}) \subset G(\mathbb{A}^f)$ be the stabilizer of $\Lambda \otimes_{\mathbb{Z}} \mathcal{O}_{\mathbb{A}^f}$. Let $h: \mathbb{S} \rightarrow G_{\mathbb{R}}$ be the unique map of real algebraic groups inducing multiplication by z^{-1} on Φ and by \overline{z}^{-1} on $\overline{\Phi}$ for an isomorphism $V \otimes_{\mathbb{Q}} \mathbb{C} \simeq \Phi \oplus \overline{\Phi}$ as F - \mathbb{C} bimodules.

Theorem (Deligne, [3], paragraph 4.12). *The coarse moduli space of strong (F, Φ) -abelian varieties with given CM datum D is the above Shimura variety.*

Now, we recall some theorems of Shimura which describe when the irreducible components of $\mathrm{Sh}_{G_{\mathcal{O}}}(G, h)$ are geometrically irreducible. To state these theorems, first observe that $\mathrm{Hom}(\mathbb{S}_{/\mathbb{C}}, \mathbb{G}_{m, \mathbb{C}})$ has for a basis the characters z and \overline{z} such that the composition $\mathbb{C}^{\times} \simeq \mathbb{S}(\mathbb{R}) \hookrightarrow \mathbb{S}(\mathbb{C}) \rightarrow \mathbb{G}_{m, \mathbb{C}} \simeq \mathbb{C}^{\times}$ is the identity and complex conjugation respectively. Write $r: \mathbb{G}_{m, \mathbb{C}} \rightarrow \mathbb{S}_{/\mathbb{C}}$ for the unique map such that $z \circ r$ is the identity and $\overline{z} \circ r$ is trivial.

Theorem (Shimura; see Deligne [3], paragraphs 3.6, 3.7, 3.9 and 3.14). *Suppose that the commutator subgroup $G' = [G, G]$ of G is simply connected. Then $\mathrm{Sh}_{G_{\mathcal{O}}}(G, h)$ is defined over K if and only if the conjugacy class of the composite map*

$$h \circ r: \mathbb{G}_{m, \mathbb{C}} \rightarrow \mathbb{S}_{\mathbb{C}} \rightarrow G_{\mathbb{C}}$$

is defined over K . Moreover, writing $T = G^{ab} = G/G'$ and $\nu: G \rightarrow T$ for the projection map, the irreducible components of $\text{Sh}_{G_{\mathcal{O}}}(G, h)$ are geometrically irreducible if and only if

$$\lambda((\text{Res}_{\mathbb{Q}}^K \mathbb{G}_{m,K})(\mathbb{A})) \subset \nu(G_{\mathcal{O}}) \cdot T(\mathbb{Q}) \cdot \nu(K_{\infty}),$$

where the map $\lambda: \text{Res}_{\mathbb{Q}}^K \mathbb{G}_{m,K} \rightarrow T$ is defined by

$$\lambda(a) = \text{Nm}_{\mathbb{Q}}^K \circ \text{Res}_{\mathbb{Q}}^K (\nu \circ h \circ r)(a^{-1}).$$

We now use these results to prove Theorem 3.11.

Proof of Theorem 3.11. By the above discussion, it suffices to show that the Shimura varieties $\text{Sh}_{G_{\mathcal{O}}}(G, h)$ are defined over K provided that Φ is defined over K , and that in this case, every irreducible component of $\text{Sh}_{G_{\mathcal{O}}}(G, h)$ is geometrically irreducible if and only if $f = \det_F \Phi$ induces the zero map $\text{Cl}(K) \rightarrow \text{Cl}^W(F)$. Note that G' is simply connected, since it is isomorphic to a special unitary group over F . Thus, we can invoke the theorems of Shimura above.

That $\text{Sh}_{G_{\mathcal{O}}}(G, h)$ is defined over K is clear: Because Φ is defined over K , the conjugacy class of $r \circ h$ is therefore defined over K .

To see that every irreducible component of $\text{Sh}_{G_{\mathcal{O}}}(G, h)$ is geometrically irreducible if and only if $f: \text{Cl}(K) \rightarrow \text{Cl}^W(F)$ is zero, we first notice that

$$T = \left\{ (x, y) \in (\text{Res}_{\mathbb{Q}}^F \mathbb{G}_{m,F}) \times \mathbb{G}_{m,\mathbb{Q}} : x \cdot \bar{x} = y^b \right\}.$$

Here, the abelianization map $\nu: G \rightarrow T$ is given explicitly by $g \mapsto (\det g, a)$, where a is the unique element of \mathbb{Q} for which $\langle gx, gy \rangle = a \cdot \langle x, y \rangle$. Under this identification, the map λ is given by

$$\lambda(a) = \left(\det_F ((x \mapsto a \cdot x): \Phi \rightarrow \Phi), \text{Nm}_{\mathbb{Q}}^K a \right).$$

Thus, the irreducible components of $\text{Sh}_{G_{\mathcal{O}}}(G, h)$ are geometrically irreducible if and only if for all $a \in K^{\times}(\mathbb{A})$, we have $\lambda(a) \subset \nu(G_{\mathcal{O}}) \cdot T(\mathbb{Q}) \cdot \nu(K_{\infty})$.

As $\nu(G_{\mathcal{O}}) = T(\mathcal{O}_{\mathbb{A}^f})$ and $\nu(K_{\infty})$ contains the connected component of $T(\mathbb{R})$, the above condition is equivalent to the assertion that for all $a \in K^{\times}(\mathbb{A})$, we can find $x \in F^{\times}$ so that $(f(a)) = (x)$ and $x \cdot \bar{x} \in (\mathbb{Q}^{\times})^b$. Since $(f(a) \cdot \overline{f(a)}) = (g(a))^b$ and $x \cdot \bar{x} > 0$, this is equivalent to $x \cdot \bar{x} \in \mathbb{Q}^{\times}$. But this is just the assertion that $f: \text{Cl}(K) \rightarrow \text{Cl}^W(F)$ is the zero map. \square

This concludes the proof of Theorem 3.11. As a corollary of Theorem 3.11, we can reprove a well-known fact about the field of definition of abelian varieties with full CM (see for example [12]).

Corollary 3.18. *If $\dim_K \Phi = \frac{[F:\mathbb{Q}]}{2}$, i.e. the CM is full, then there exists an (F, Φ) -abelian variety B defined over $K_{F,\Phi}$.*

Proof. In this case the Shimura variety $\mathrm{Sh}_{G_{\mathcal{O}}}(G, h)$ is zero-dimensional, hence any geometrically irreducible component over $K_{F, \Phi}$ corresponds to a single (strong) (F, Φ) -abelian variety whose field of moduli is $K_{F, \Phi}$. Moreover, by [11], this abelian variety can be defined over its field of moduli. \square

Finally, using a theorem of Rizov, we have:

Corollary 3.19. *The intersection of all fields K over which one can define an (F, Φ) -abelian variety is $K_{F, \Phi}$.*

Proof. This follows from Theorem 3.11 by a theorem of Rizov [15]. \square

4 Associated Characters of $A[\ell]$: Local Properties

In this section, we give some local properties of the associated characters of $A[\ell]$, most importantly Lemmas 4.3 and 4.11, and Corollary 4.7.

4.1 Action of Frobenius Elements

Fix a prime $v \nmid \ell$. If A has good reduction at v , then ρ_{A, ℓ^∞} is unramified at v and the Frobenius element at v acts by a matrix whose characteristic polynomial P_v is defined over \mathbb{Z} , and which has the additional property that all roots of P_v have (complex) norm $\sqrt{|\mathrm{Nm}(v)|}$. (Note that this implies a bound on the coefficients of P_v given v .) When instead of ρ we consider an associated character ψ , this implies that ψ at a prime of good reduction is unramified, and the image of a Frobenius element satisfies a polynomial all of whose roots are a product of d roots of P_v .

When we drop the assumption that v has good reduction, the character ψ can become ramified at v , but a very similar result still holds — in particular, the image under ψ of any Frobenius element π of v satisfies one of a finite set (depending on v) of polynomials with integral coefficients. Namely, we have the following result of Grothendieck.

Lemma 4.1 (Grothendieck). *Let $v \in \Sigma_K \setminus \Sigma_\ell$ be any prime not dividing ℓ . Then for any choice of Frobenius element $\pi = \pi_v \in G_K$ extending frob_v , the characteristic polynomial P_π of π acting on the ℓ -adic Tate module $A[\ell^\infty]$ has the following properties.*

1. *The coefficients of P_π are integers, and are independent of ℓ .*
2. *Every root of P_π has magnitude that does not depend on the choice of complex embedding, and is equal to 1, the norm of v , or the square root of the norm of v .*
3. *The roots of P_π come in pairs which multiply to the norm of v .*

Proof. Properties 1 and 2 are Theorem 4.3(b) and Corollary 4.4 in [6] respectively; property 3 follows from the Galois-invariance of the Weil pairing. \square

Note that $\psi(\pi)$ is the product of some subset of eigenvalues of $\rho_{A,\ell}(\pi)$. In light of the above lemma, this means that $\psi(\pi)$ is the reduction modulo some prime ideal $\mathfrak{l} \subset \mathcal{O}_{\overline{\mathbb{Q}}}$ lying over ℓ of a product of d roots of P_v in $\overline{\mathbb{Q}}$.

Definition 4.2. For any prime v of K , choose a Frobenius element π over v and define

$$\psi_{\mathbb{C}}(v) \in \overline{\mathbb{Q}}$$

to be a product of d distinct roots of P_{π} such that $\psi(\pi) \equiv \psi_{\mathbb{C}}(v) \pmod{\mathfrak{l}}$ (There may be several choices for $\psi_{\mathbb{C}}(v)$, but at least one exists by the above lemma. We make such a choice for each v .)

Lemma 4.3. *For any prime ideal $v \nmid \ell$, there are only finitely many possible values of $\psi_{\mathbb{C}}(v)$, all of which are algebraic of degree at most $\binom{2g}{d}$. Moreover, there is some integer a with $0 \leq a \leq 2d$ such that under any complex embedding,*

$$|\psi_{\mathbb{C}}(v)| = \sqrt{|\mathrm{Nm}_{\overline{\mathbb{Q}}}^K(v)|^a}.$$

Proof. This is a direct consequence of Lemma 4.1. (To see that $\psi_{\mathbb{C}}(v)$ is algebraic of degree at most $\binom{2g}{d}$, note that any conjugate of $\psi_{\mathbb{C}}(v)$ in $\overline{\mathbb{Q}}$ is a product of d roots of the Frobenius polynomial $P_{\pi} \in \mathbb{Z}[x]$, and in particular there are at most $\binom{2g}{d}$ of them.) \square

4.2 Semistable Reduction

It is well known that any abelian variety A becomes semistable after a finite extension of the ground field. In order to analyze the local action of $\rho_{A,\ell}$ in Section 4.3, we will need to make some more precise statements, which let us control the ramification in a careful way.

Definition 4.4. We define the constant c_g to be the least common multiple of all integers n such that for all but (at most) one odd prime p , the symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_p)$ has an element of order n .

Remark 4.5. For an alternative definition of c_g , see Theorem 7.2.

Lemma 4.6. *Let v be a valuation on K . Then there exists a (finite and Galois) extension L of K such that A acquires semistable reduction at v over L and the exponent of the inertia subgroup at v of $\mathrm{Gal}(L/K)$ divides c_g .*

Proof. For any odd prime p distinct from the residue characteristic of v , write $L^{(p)}$ for the field obtained by adjoining the p -torsion points of A to K . By Proposition 4.7 of [6], A acquires semistable reduction over each $L^{(p)}$.

For any set S of prime numbers, define $c_S(g)$ to be the least common multiple of all integers n such that for all odd primes $p \in S$, the symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_p)$ has an element of order n . Clearly, we can select some finite set $S = \{p_1, p_2, \dots, p_k\}$ of primes, all distinct

from the residue characteristic of v , so that $c_S(g) = c_g$. Moreover, we can select this set of primes such that none of them divide the degree of some fixed polarization of A .

Write $F = L^{(p_1)} \cdot L^{(p_2)} \cdots L^{(p_k)}$ for the composite field, and $I \subset \text{Gal}(F/K)$ for the inertia subgroup at v . Define $L \subset F$ to be the fixed field of the subgroup generated by the kernels of the restriction maps on I , i.e.

$$L = \text{fixed field of } \left(\left\langle \ker \left(I \rightarrow \text{Gal}(L^{(p_i)}/K) \right) : i = 1, 2, \dots, k \right\rangle \subset \text{Gal}(F/K) \right).$$

Then an element of $\text{Gal}(L/K)$ is the image of an element in $\text{Gal}(L^{(p_i)}/K)$ for any i , so its order divides c_g . To see that A acquires good reduction over L , fix some prime q distinct from the residue characteristic of v and all of the p_i .

As proved in subsection 4.1 of [6], the subset $I' \subset I$ of elements which act unipotently on the Tate module $T_q A$ forms a normal subgroup. Proposition 3.5 of [6] implies that for all p_i , the kernel $\ker(I \rightarrow \text{Gal}(L^{(p_i)}/K))$ acts unipotently on $T_q A$; hence the kernel belongs to I' . Thus, the subgroup spanned by the kernels belongs to I' , and therefore acts unipotently on $T_q A$. Applying Proposition 3.5 of [6] again, we see that A acquires semistable reduction at v over L . \square

Corollary 4.7. *The character ψ^{c_g} is unramified at all places v not lying over ℓ .*

Proof. By Proposition 3.5 of [6], $\rho_{A,\ell,L}$ is unramified at v if v is semistable for A over L . Now $g^{c_g} \in G_L \subset G_K$ for any $g \in G_K$, hence the corollary. \square

Lemma 4.8. *Let $v \mid \ell$, and suppose $\ell \nmid c_g$. Then, for any abelian variety A , there exists an extension L_w/K_v over which A acquires semistable reduction and such that $[L_w : K_v] \mid c_g$.*

Proof. Write L^0 for the field L given by Lemma 4.6, and let w_0 be an extension of v to L^0 . Since $\ell \nmid c_g$, it follows that $L_{w_0}^0/K_v$ is tamely ramified. In particular, its inertia subgroup is cyclic. Thus, the order e of its inertia subgroup divides c_g .

Write $I_v \subset G_v = \text{Gal}(\overline{K_v}/K_v)$ for the inertia subgroup and $G_{\text{res}} = \text{Gal}(\overline{k_v}/k_v)$ for the Galois group of the residue field. Note that there are noncanonical splittings $G_{\text{res}} \rightarrow G_v$ making G_v into a semidirect product of I_v and G_{res} . Fix such a splitting. Now if H_0 is the normal subgroup corresponding to $L_{w_0}^0$ then $H_0 \cap I_v$ is normal in G_v and we can take for L_w the field corresponding to the (not necessarily normal) subgroup $H_0 \cap I_v \times G_{\text{res}}$. \square

Remark 4.9. Since in what follows we will only be interested in the action of I_v , one could also work with the extension $K_v^{nr} \cdot L_w^0/K_v^{nr}$ instead of having to choose a splitting and working with L_w/K_v . We will use the essentially equivalent pair L_w/K_v to avoid dealing with infinite p -adic extensions.

4.3 Action of Inertia Groups

Suppose at first that $v \mid \ell$ is semistable for A . Then a remarkable result of Raynaud [14] shows that the associated characters of ρ_ℓ restricted to I_v are algebraic over ℓ in the sense of section 2.

Lemma 4.10. *If A has semistable reduction at $v \mid \ell$, then $\psi|_{I_v}$ is the reduction of a negative algebraic character of degree at most d times the ramification index of v .*

Proof. As explained in [6], subsection 2.2.3, we have a canonically defined subrepresentation $A[\ell]^f \subset A[\ell]$ which comes from a finite flat commutative group scheme over $\text{Spec } \mathcal{O}_{K_v}$. Thus, when restricted to the inertia subgroup, the associated character ψ decomposes as a product of at most d associated characters of $A[\ell]^f$ and of the quotient $A[\ell]/A[\ell]^f$. For the associated characters of $A[\ell]^f$, we are done by Corollary 3.4.4 of [14]. On the other hand, Proposition 5.6 of [6] implies that the action of the Galois group on $A[\ell]/A[\ell]^f$ is unramified at v , i.e., each associated character of the restriction to the inertia subgroup is trivial. \square

Lemma 4.11. *Let $v \mid \ell$, and suppose $\ell \nmid \Delta_K \cdot c_g$. Then, for any abelian variety A , the restriction $\psi^{c_g}|_{I_v}$ is the reduction of a negative algebraic character of degree at most $d \cdot c_g$.*

Proof. Let L_w be the field given by Lemma 4.8; write $e = [L_w : K_v]$. Functoriality of class field theory tells us that the map $\rho_{A,\ell}: \mathcal{O}_{L_w}^\times \rightarrow \overline{\mathbb{F}}_\ell^\times$ giving the action of $\text{Gal}(L^{\text{ab}}/L)$ on $A[\ell]$ is defined by composition with the norm map $\text{Nm}_{K_v}^{L_w}: \mathcal{O}_{L_w}^\times \rightarrow \mathcal{O}_{K_v}^\times$, as follows

$$\begin{array}{ccc}
 \mathcal{O}_{K_v}^\times & \xrightarrow{\quad} & \mathcal{O}_{L_w}^\times \\
 \searrow \wr \mapsto \wr^e & & \downarrow \text{Nm}_{K_v}^{L_w} \\
 & & \mathcal{O}_{K_v}^\times \xrightarrow{\quad \psi \quad} \overline{\mathbb{F}}_\ell^\times \\
 & & \nearrow \wr \\
 & & \mathcal{O}_{L_w}^\times
 \end{array}$$

Since $\ell \nmid \Delta_K$, the ramification index of w is at most e . In addition, for any $u \in \mathcal{O}_{K_v}^\times$, we have

$$\psi(u)^{c_g} = \psi(u^e)^{c_g/e} = \psi\left(\text{Nm}_{K_v}^{L_w} u\right)^{c_g/e}$$

which is the reduction of a negative algebraic character of degree at most $d \cdot c_g$ by Lemma 4.10. \square

5 Associated Characters of $A[\ell]$: Global Analysis

In this section, we will patch the local information from the previous section together into global information in order to deduce the main theorem.

Remark 5.1. In fact, we will prove the main theorem using only Lemmas 4.3 and 4.11, and Corollary 4.7 from the previous section (as well as the fact that c_g is even). In particular, this means that the conclusion of the main theorem holds more generally for any Galois character satisfying these three results. (When we make the main theorem effective in Section 7, we will for concreteness use the more explicit Lemma 4.1 as well.)

5.1 The Character θ^S

For the remainder of the paper, we can assume $\ell \nmid c_g \cdot \Delta_K$. Together, the data of ψ at all inertia groups lets us reconstruct ψ^{c_g} on the subgroup of G_K fixing the Hilbert class field. Namely let $U \subset \mathbb{I}$ be the group of units.

Lemma 5.2. *There is a positive algebraic character θ^F of degree at most $d \cdot c_g$ such that the restriction $\psi^{c_g}|_U \equiv (\theta_\ell^F)^{-1} \pmod{\mathfrak{l}}$.*

Proof. This is an immediate consequence of Lemma 4.11 and the fact that ψ^{c_g} is unramified at $v \nmid \ell$ (by Lemma 4.7). (Note that since c_g is even, we don't need to worry about the infinite places.) \square

Definition 5.3. We say that a pair (S, e) , where $e \mid c_g$ and $S \in \mathbb{Z}[\Gamma_K]$ is of degree $d \cdot e$ *corresponds* to an associated character ψ if for all $x \in K^\times$ be relatively prime to ℓ ,

$$\psi(x_\ell)^{c_g} \equiv \theta^S(x)^{c_g/e} \pmod{\mathfrak{l}}.$$

If e is coprime to S as an element of $\mathbb{Z}[\Gamma_K]$, we say that (S, e) is *reduced*.

Lemma 5.4. *Every associated character corresponds to a reduced pair (S, e) . (When A is semistable at all primes lying over ℓ , we can take $e = 1$.)*

Proof. Let $F \in \mathbb{Z}[\Gamma_K]$ be the index from Lemma 5.2. Define f to be the greatest common divisor of c_g and the F , and write $e = c_g/f$. By Lemma 4.10, $e = 1$ when A is semistable at all primes over ℓ . We define

$$S = \frac{F}{f} \in \mathbb{Z}[\Gamma_K].$$

Since $\psi(x_\ell) \cdot \psi(x_\ell) = 1$ for $x \in K^\times$, and $\theta^F(x) = (\theta^S(x))^{c_g/e}$, we are done by Lemma 5.2. \square

5.2 Analysis of the Character θ^S

Definition 5.5. We adopt the notation “ ℓ sufficiently large” to mean “ ℓ larger than a constant depending only on K and g .”

For the rest of this section, we fix K and one of the $(d \cdot c_g + 1)^{n_K}$ possible reduced pairs (S, e) , and we assume (S, e) corresponds to an associated character of an abelian variety. Here we will give ineffective bounds; we will make these arguments effective in section 7.

Lemma 5.6. *For ℓ sufficiently large, the character θ^S is balanced.*

Proof. If the character θ^S is not balanced, then there is some unit u for which $\theta^S(u)$ is not a root of unity by Lemma 2.15. However, we have

$$\theta^S(u)^{c_g/e} \equiv \psi(u_{\widehat{\ell}})^{c_g} \equiv 1 \pmod{\mathfrak{l}}$$

which is a contradiction for ℓ sufficiently large. \square

Definition 5.7. We define h'_K to be the exponent of the class group $\text{Cl}(K)$.

Lemma 5.8. *Let v be a prime ideal. As $v^{h'_K}$ is principal, we can write $v^{h'_K} = (x)$. Then if ℓ is sufficiently large relative to v , we have*

$$\psi_{\mathbb{C}}(v)^{c_g \cdot h'_K} = \theta^S(x)^{c_g/e}.$$

Proof. If ℓ is sufficiently large relative to v , then v does not lie over ℓ . Thus, for any choice of Frobenius element π_v at v , Lemma 5.4 implies

$$\psi\left(\pi_v^{h'_K}\right)^{c_g} \equiv \theta^S(x)^{c_g/e} \pmod{\mathfrak{l}}. \quad (4)$$

Hence ℓ divides the norm of their difference. By Lemma 4.3, there are only finitely many possibilities for the left-hand side as A ranges over all abelian varieties of dimension g . So if ℓ is sufficiently large, then we have the desired equality. \square

Lemma 5.9. *For ℓ sufficiently large, there is a fixed integer a with $0 \leq a \leq 2d$ such that if σ and τ are complex conjugate embeddings (for any choice of embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$), then*

$$S(\sigma) + S(\tau) = ae.$$

Proof. In light of Lemma 5.6, there is an integer a' such that $S(\sigma) + S(\tau) = a'$ for any complex conjugate embeddings σ and τ . Hence, it suffices to show that this integer a' satisfies $a' = a \cdot e$ for a an integer with $0 \leq a \leq 2d$.

Let v be a prime ideal of K , and write $v^{h'_K} = (x)$. From Lemma 4.3, there exists some integer a with $0 \leq a \leq 2d$ such that under any complex embedding,

$$|\psi_{\mathbb{C}}(v)| = \sqrt{|\text{Nm}_{\mathbb{Q}}^K(v)|}^a.$$

On the other hand, under any complex embedding, we have

$$|\theta^S(x)| = \sqrt{|\text{Nm}_{\mathbb{Q}}^K(x)|}^{a'} = \sqrt{|\text{Nm}_{\mathbb{Q}}^K(v)|}^{a' \cdot h'_K}.$$

By Lemma 5.8, we have

$$\psi_{\mathbb{C}}(v)^{c_g \cdot h'_K} = \theta^S(x)^{c_g/e} \quad \Rightarrow \quad \psi_{\mathbb{C}}(v)^{e \cdot c_g \cdot h'_K} = \theta^S(x)^{c_g}$$

Combining these, we have

$$\sqrt{|\mathrm{Nm}_{\mathbb{Q}}^K(v)|}^{a \cdot e \cdot c_g \cdot h'_K} = |\psi_{\mathbb{C}}(v)|^{e \cdot c_g \cdot h'_K} = |\theta^S(x)|^{c_g} = \sqrt{|\mathrm{Nm}_{\mathbb{Q}}^K(v)|}^{a' \cdot c_g \cdot h'_K}.$$

Hence $a' = a \cdot e$, which is what we wanted to show. \square

Definition 5.10. We define $F \subset \overline{\mathbb{Q}}$ to be the smallest field containing the image of θ^S .

Lemma 5.11. *Let $v \in \mathcal{O}_K$ be degree 1 and unramified in K/\mathbb{Q} . Then there is no factor e' of e such that $\theta^S(v)$ is an (e') th power in the group of ideals of F .*

Proof. By assumption, the set of exponents to which primes occur in the prime factorization of $\theta^S(v)$ are the same as coefficients of S . In particular, e is coprime to the greatest common divisor of all these coefficients. \square

Lemma 5.12. *Let ℓ be sufficiently large; suppose that $v \in \mathcal{O}_K$ is a prime ideal of degree 1, unramified in K/\mathbb{Q} . Write $v^{h'_K} = (x)$. Then $\theta^S(x)^{c_g/e}$ generates F over \mathbb{Q} .*

Proof. Take any $\tau \in \mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q})$ which fixes $\theta^S(x)^{c_g/e}$. We want to show that τ fixes the field F . Since τ fixes $\theta^S(x)^{c_g/e}$, we have an equality of ideals of K^{gal} :

$$\left(\prod_{\sigma \in \Gamma_K} \sigma(v)^{S(\sigma)} \right)^{h'_K \cdot c_g/e} = \left(\prod_{\sigma \in \Gamma_K} \tau\sigma(v)^{S(\sigma)} \right)^{h'_K \cdot c_g/e}.$$

Since the group of ideals of K^{gal} is torsion-free, this implies

$$\prod_{\sigma \in \Gamma_K} \sigma(v)^{S(\sigma)} = \prod_{\sigma \in \Gamma_K} \tau\sigma(v)^{S(\sigma)} = \prod_{\sigma \in \Gamma_K} \sigma(v)^{S(\tau^{-1}\sigma)}.$$

Because v is an unramified prime of degree 1, its images under distinct embeddings into K^{gal} generate coprime ideals of K^{gal} . Hence, by the uniqueness of prime factorization into ideals for K^{gal} , we have $S(\sigma) = S(\tau^{-1}\sigma)$ for all $\sigma \in \Gamma_K$. Thus, for any $z \in K^\times$, we have

$$\theta^S(z) = \prod_{\sigma \in \Gamma_K} \sigma(z)^{S(\sigma)} = \prod_{\sigma \in \Gamma_K} \sigma(z)^{S(\tau^{-1}\sigma)} = \prod_{\sigma \in \Gamma_K} \tau\sigma(z)^{S(\sigma)} = \tau\theta^S(z),$$

so τ fixes the image of θ^S and hence the field F . \square

In particular, the above lemma together with Lemma 4.3 implies that for ℓ sufficiently large, F has degree at most $\binom{2g}{d}$. In fact, we can prove a stronger statement.

Lemma 5.13. *If ℓ is sufficiently large, then for any ideal class $\mathfrak{v} \in \mathrm{Cl}(K)$,*

$$\mathrm{ord}_{\mathrm{Cl}^W(F)}(C\theta^S(\mathfrak{v})) \cdot [F : \mathbb{Q}] \cdot e \leq \binom{2g}{d}.$$

Proof. By the Chebotarev Density Theorem, we can find some prime ideal $v \subset \mathcal{O}_K$ representing the ideal class \mathfrak{v} which is of degree 1 and unramified in K/\mathbb{Q} (since the set of prime ideals of degree greater than 1 or ramified in K/\mathbb{Q} has density zero). Write $v^{h'_K} = (x)$. By Lemma 5.8,

$$\psi_{\mathbb{C}}(v)^{c_g \cdot h'_K} = \theta^S(x)^{c_g/e}. \quad (5)$$

By Lemma 4.3, $\psi_{\mathbb{C}}(v)$ lies in some field L of degree at most $\binom{2g}{d}$. However, by Lemma 5.12, the right-hand side generates the field F over \mathbb{Q} . Thus, we have $F \subset L$. Hence, we have an equality of ideals of L :

$$(\psi_{\mathbb{C}}(v))^{c_g \cdot h'_K} = (\theta^S(x)^{c_g/e}) = \theta^S(v)^{c_g \cdot h'_K/e}.$$

Because the group of fractional ideals is torsion-free, $(\psi_{\mathbb{C}}(v))^e = \theta^S(v)$. Taking norm down to F , we have an equality of ideals of F

$$(\mathrm{Nm}_F^L \psi_{\mathbb{C}}(v))^e = (\theta^S(v))^{[L:F]}.$$

Since the left-hand side is an e th power in the group of ideals, the right-hand side must be as well; thus $e \mid [L : F]$ by Lemma 5.11. Because the group of ideals is torsion-free,

$$(\mathrm{Nm}_F^L \psi_{\mathbb{C}}(v)) = (\theta^S(v))^{\frac{[L:F]}{e}}.$$

The left-hand side is zero in $\mathrm{Cl}^W(F)$, so the right-hand side is too. This gives

$$\mathrm{ord}_{\mathrm{Cl}^W(F)}(\theta^S(v)) \leq \frac{[L : F]}{e} = \frac{[L : \mathbb{Q}]}{[F : \mathbb{Q}] \cdot e} \leq \frac{\binom{2g}{d}}{[F : \mathbb{Q}] \cdot e},$$

which implies the desired inequality. \square

Lemma 5.14. *There exists an integer N divisible by eN_0 (recall that N_0 is the number of roots of unity in F) and satisfying $\varphi(N) \leq \binom{2g}{d}$ such that when restricted to $\mathrm{Gal}(\overline{K}/K_{F,\Phi})$,*

$$(\psi|_{\mathrm{Gal}(\overline{K}/K_{F,\Phi(S)})})^{e \cdot w} = \psi_{F,\Phi(S)}^w \quad \text{where} \quad w = \frac{1}{e} \cdot \mathrm{lcm}(N, c_g).$$

Proof. Define

$$\chi = (\psi|_{\mathrm{Gal}(\overline{K}/K_{F,\Phi(S)})})^{e \cdot N_0} \otimes \psi_{F,\Phi(S)}^{N_0} \quad \text{and} \quad w_0 = \frac{c_g}{\mathrm{gcd}(eN_0, c_g)}.$$

From Lemma 4.7, it follows that χ^{w_0} is unramified at all places not lying over ℓ . By assumption, it is trivial at all idèles of the form $x_{\hat{\ell}}$ for $x \in K^\times$ relatively prime to ℓ . It follows that χ^{w_0} is trivial on $\mathrm{Gal}(\overline{K}/H_K)$ (by the idèlic formulation of class field theory). That is, χ^{w_0} gives a well-defined character $\chi^{w_0} : \mathrm{Gal}(H_K/K_{F,\Phi}) \rightarrow \overline{\mathbb{F}}_\ell^\times$.

Let \mathfrak{v} be an ideal class such that $\chi^{w_0}(\mathfrak{v})$ generates the image of χ^{w_0} in $\overline{\mathbb{F}}_\ell^\times$. Let v be a prime ideal representing \mathfrak{v} which is of degree 1, does not divide $h'_K \cdot c_g$, and is unramified in K/\mathbb{Q} . Note that by definition,

$$\chi(\pi_v) = X^{N_0} \quad \text{for} \quad X = \frac{\psi_{\mathbb{C}}(v)^e}{g},$$

where $g \in F^\times$ is any Weil number such that $\theta^S(v) = (g)$.

Lemma 5.8 implies that $X^{h'_K \cdot c_g} = 1$ for ℓ sufficiently large. Note that by Lemma 5.12, $F \subset \mathbb{Q}[\pi_{\mathbb{C}}(v)^e]$, so $\mathbb{Q}[X] \subset \mathbb{Q}[\psi_{\mathbb{C}}(v)^e] \cdot F \subset \mathbb{Q}[\psi_{\mathbb{C}}(v)^e]$.

By Lemma 5.11, there is no factor e' of e for which $(g) = \theta^S(v)$ is an (e') th power in the group of ideals of F . But Lemma 5.8 implies that $\psi_{\mathbb{C}}(\pi_v)^e$ equals g times an $(h'_K \cdot c_g)$ th root of unity, so $\mathbb{Q}[\psi_{\mathbb{C}}(\pi_v)^e]/F$ is unramified at all primes dividing $\theta^S(v)$. Hence, there is no factor e' of e for which $(\psi_{\mathbb{C}}(v)^e) = (g)$ is an (e') th power in the group of ideals of $\mathbb{Q}[\psi_{\mathbb{C}}(v)^e]$. This implies that $[\mathbb{Q}[\psi_{\mathbb{C}}(v)] : \mathbb{Q}[\psi_{\mathbb{C}}(v)^e]] = e$. Hence, Lemma 4.3 gives

$$[\mathbb{Q}[X] : \mathbb{Q}] \leq [\mathbb{Q}[\psi_{\mathbb{C}}(v)^e] : \mathbb{Q}] = \frac{1}{e} \cdot [\mathbb{Q}[\psi_{\mathbb{C}}(v)] : \mathbb{Q}] \leq \frac{1}{e} \cdot \binom{2g}{d}.$$

Since $\varphi(em) \leq e\varphi(m)$, we can take N to be e times the number of roots of unity in $\mathbb{Q}[X]$. By construction, $eN_0 \mid N$ and $X^{N/e} = 1$, so

$$(\psi|_{\text{Gal}(\overline{K}/K_{F,\Phi(S)})})^{e \cdot w} = \psi_{F,\Phi(S)}^w \quad \text{where} \quad w = \gcd(N/e, N_0 \cdot w_0) = \frac{1}{e} \cdot \text{lcm}(N, c_g). \quad \square$$

Theorem 5.15. *Let K be a number field and g and d be positive integers. Suppose ℓ is a prime number not belonging to some finite set $S_{K,g}$ depending only on K and g . Suppose moreover that A is a g -dimensional abelian variety defined over K and ψ_0 is an associated character of $\rho_{A,\ell}$ of degree d . Then, for an effectively computable integer $c_g < 12^{4g^2}$, there is a positive algebraic character θ^S and positive integer e such that the following conditions are satisfied.*

1. *The character θ^S is balanced, of total degree $a \cdot e$ for some $0 \leq a \leq 2d$.*
2. *The induced map $C\theta^S : \text{Cl}(K) \rightarrow \text{Cl}^W(F)$ is trivial, i.e. $K \supset K_{F,\Phi(S)}$.*
3. *There exists an integer N divisible by eN_0 and satisfying $\varphi(N) \leq \binom{2g}{d}$ such that*

$$\psi^{e \cdot w} = \psi_{F,\Phi(S)}^w \quad \text{where} \quad w = \frac{1}{e} \cdot \text{lcm}(N, c_g).$$

4. *We have the inequality $[F : \mathbb{Q}] \cdot e \leq \binom{2g}{d}$.*

Proof. Write e' for the exponent of the induced map $C\theta^S : \text{Cl}(K) \rightarrow \text{Cl}^W(F)$. Then, after replacing (S, e) with $(S \cdot e', e \cdot e')$, this follows from Lemmas 5.9, 5.13 and 5.14. \square

5.3 Proof of Main Theorem

Theorem 5.16. *Let K be a number field, and g and d be positive integers. Then, there exists a finite set $S_{K,g}$ of prime numbers depending only on K and g , and a constant $0 < c_g < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g -dimensional abelian variety A with a mod- ℓ associated character ψ_0 of degree d , we have*

$$\psi^{e \cdot w} \equiv \psi_{F,\Phi}^w \pmod{\ell},$$

where ψ is either ψ_0 or $\text{cyc}_\ell^d \otimes \psi_0^{-1}$ and $w = \frac{\text{lcm}(N, c_g)}{\text{gcd}(e, c_g)}$. Here, F is either \mathbb{Q} or a CM-field, and $\Phi: F \rightarrow \text{End}(K^m)$ is a primitive balanced representation such that $K \supset K_{F,\Phi}$. The quantities a , e , and N are integers with e and N positive, which satisfy $m = \frac{1}{2} \cdot a \cdot e \cdot [F : \mathbb{Q}]$. Moreover, $0 \leq a \leq d$, and both $\varphi(N)$ and $e \cdot [F : \mathbb{Q}]$ are at most $\binom{2g}{d}$.

Proof. Let (S, e) corresponding to ψ be as in Theorem 5.15. Note that (S', e) corresponds to $\text{cyc}_\ell^d \otimes \psi^{-1}$, where S' is defined by $S'(\sigma) = de - S(\sigma)$. One can easily check that (S', e) satisfies the conclusion of Theorem 5.15 for the character $\text{cyc}_\ell^d \otimes \psi^{-1}$. Thus, by replacing ψ with $\text{cyc}_\ell^d \otimes \psi^{-1}$ if necessary, we may suppose that $0 \leq a \leq d$.

Let Φ be the representation of F such that $\det_F \Phi = \theta^S$ (see Proposition 3.6). By construction, $\dim \Phi = \frac{1}{2} \cdot [F : \mathbb{Q}] \cdot a \cdot e$. The conclusion of this theorem then follows from Theorem 5.15. \square

Theorem 5.17. *In Theorem 5.16, if we assume in addition that A is semistable at primes lying over ℓ , then we can take $e = 1$, provided that we weaken the conclusion to be that $\psi^w = \psi_{F,\Phi}^w$ on $\text{Gal}(\overline{K}/K \cdot K_{F,\Phi})$ and*

$$[F : \mathbb{Q}] \cdot (\text{exponent } K \cdot K_{F,\Phi}/K) \leq \binom{2g}{d}.$$

Proof. We use the same argument as in the proof of Theorem 5.16, without replacing (S, e) by $(e' \cdot S, e' \cdot e)$. Instead, we replace K with the unramified abelian extension M of K defined by the kernel of $C\theta^S: \text{Cl}(K) \rightarrow \text{Cl}^W(F)$. \square

5.4 Some Corollaries of the Main Theorem

Corollary 5.18. *Let K be a number field that does not contain any CM-fields (which is in particular true when K has a real embedding), and g and d be positive integers. There exists a finite set $S_{K,g}$ of prime numbers depending only on K and g , and a constant $0 < c_g < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g -dimensional abelian variety A with a mod- ℓ associated character ψ of degree d ,*

$$\psi^{2w} = \text{cyc}_\ell^{aw},$$

where a is an integer with $0 \leq a \leq 2d$, and $w = \frac{\text{lcm}(c_g, N)}{2}$ for some positive $N \leq \binom{2g}{d}$.

Proof. Since $K \supset K_{F,\Phi}$ and $K_{F,\Phi}$ contains a CM-field when F is a CM-field, F cannot be a CM-field. Thus, $F = \mathbb{Q}$, which gives the desired conclusion. \square

Corollary 5.19. *Let K be a number field, and g and d be positive integers. Then, there exists a finite set $S_{K,g}$ of prime numbers depending only on K and g , and a constant $0 < c_g < 12^{4g^2}$ depending only on g such that, for a prime $\ell \notin S_{K,g}$, and a g -dimensional abelian variety A with a mod- ℓ associated character ψ of degree 1, one of the following holds.*

1. *The character ψ^{c_g} is trivial or equal to $\text{cyc}_\ell^{c_g}$.*
2. *There exists an abelian unramified extension M/K , a (full) CM abelian variety A' defined over M , such that K contains the reflex field of the CM field of A' (which in particular implies that A' has CM defined over M), and an ℓ -adic associated character of degree 1 of A' , whose mod- ℓ reduction ψ' satisfies*

$$(\psi|_{\text{Gal}(\overline{K}/M)})^{c_g} = (\psi')^{c_g} \quad \text{and} \quad (\dim A') \cdot (\text{exponent } M/K) \leq g.$$

Proof. Here, we use Theorem 5.17. The two cases correspond to $F = \mathbb{Q}$ and F a CM-field. In the second case, we have $m = \frac{1}{2} \cdot [F : \mathbb{Q}]$, so the result follows from Corollary 3.18. \square

The next two Corollaries list the possible degree 1 associated characters for $g \in \{2, 3\}$. (Note that the easiest way of computing c_g is to use Theorem 7.2 of Section 7 below.)

Corollary 5.20. *Let K be a number field. Then there exists a finite set $S_{K,2}$ of prime numbers depending only on K such that, for a prime $\ell \notin S_{K,2}$, and an abelian surface A with a mod- ℓ associated character ψ of degree 1, one of the following holds.*

1. *There exists a full CM abelian surface A' over K whose CM is defined over K , with an ℓ -adic degree 1 associated character whose mod- ℓ reduction ψ' satisfies*

$$\psi^{120} = (\psi')^{120}.$$

2. *There exists an abelian unramified extension L/K of exponent at most 2, a CM elliptic curve E' defined over L , such that K contains the CM field, and an ℓ -adic degree 1 associated character of E' whose mod- ℓ reduction ψ' satisfies*

$$\psi|_{\text{Gal}(\overline{K}/L)}^{120} = (\psi')^{120}.$$

3. *For some $a \in \{0, 60, 120\}$, we have*

$$\psi^{120} = \text{cyc}_\ell^a.$$

Corollary 5.21. *Let K be a number field. Then there exists a finite set $S_{K,3}$ of prime numbers depending only on K such that, for a prime $\ell \notin S_{K,3}$, and an abelian threefold A with a mod- ℓ associated character ψ of degree 1, one of the following holds.*

1. *There exists a full CM abelian surface or threefold A' over K whose CM is defined over K , with an ℓ -adic degree 1 associated character whose mod- ℓ reduction ψ' satisfies*

$$\psi^{2520} = (\psi')^{2520}.$$

2. *There exists an abelian unramified extension L/K of exponent at most 3, a CM elliptic curve E' defined over L , such that K contains the CM field, and an ℓ -adic degree 1 associated character of E' whose mod- ℓ reduction ψ' satisfies*

$$\psi|_{\text{Gal}(\overline{K}/L)}^{2520} = (\psi')^{2520}.$$

3. *There exists a CM elliptic curve E' over K , such that K contains the CM field, and an ℓ -adic degree 1 associated character of E' whose mod- ℓ reduction ψ' satisfies*

$$\psi^{2520} = (\psi' \otimes \text{cyc}_\ell)^{840}.$$

4. *For some $a \in \{0, 1260, 2520\}$, we have*

$$\psi^{2520} = \text{cyc}_\ell^a.$$

6 The Special Case of Elliptic Curves

In this section, we assume in addition that $g = 1$, i.e. that $A = E$ is an elliptic curve. In this case, we can prove a slightly stronger theorem.

6.1 Theorem 5.16 in the Case $g = 1$

Lemma 6.1. *Let K be a number field. Then, there exists a finite set S_K of prime numbers depending only on K such that, for a prime $\ell \notin S_K$, and an elliptic curve E over K for which $E[\ell] \otimes \overline{\mathbb{F}}_\ell$ is reducible with degree 1 associated character ψ , one of the following holds.*

1. *We have $\psi^{12} \in \{1, \text{cyc}_\ell^6, \text{cyc}_\ell^{12}\}$.*
2. *There exists a CM elliptic curve E' , which is defined over K and whose CM-field is contained in K , with an ℓ -adic degree 1 associated character whose mod- ℓ reduction ψ' satisfies:*

$$\psi^{12} = (\psi')^{12}$$

Proof. If $F = \mathbb{Q}$ in Theorem 5.16, Case 1 holds. Otherwise, F is imaginary quadratic, and we can take $E' = \mathbb{C}/\mathcal{O}_F$, since $\psi_{F,\Phi} = \psi'$ and $K_{F,\Phi}$ is the Hilbert class field of F . \square

6.2 Effective Chebotarev Theorem

Under GRH, we have the following effective version of the Chebotarev Density Theorem, due to Lagarias and Odlyzko, with improvements due to Bach.

Theorem (Effective Chebotarev). *Let E/K be a Galois extension of number fields with $E \neq \mathbb{Q}$. Then under GRH, there exists an effectively computable absolute constant c_5 such that every conjugacy class of $\text{Gal}(E/K)$ is represented by a Frobenius element of a prime ideal $v \in \Sigma_K$ which is unramified in E , such that*

$$\text{Nm}_{K/\mathbb{Q}}(v) \leq c_5(\log \Delta_E)^2.$$

Moreover, we can take v to be a prime of degree 1 and unramified in K/\mathbb{Q} .

Proof. See [7], remark at end of paper regarding the improvement to Corollary 1.2. That we can take \mathfrak{p} to be of degree 1 and unramified in K/\mathbb{Q} follows from Theorem 3.1 in [1]. \square

Remark 6.2. Unconditionally, a similar theorem is true, with the bound of $c_5(\log \Delta_E)^2$ replaced by $\exp(c_6 \Delta_E)$, for an effectively computable absolute constant c_6 .

In fact, we will need a very slight strengthening of the above Theorem, to avoid possible issues at the prime 3.

Corollary 6.3. *Let E/K be a Galois extension of number fields with $E \neq \mathbb{Q}$, and let N be a positive (rational) integer. Then under GRH, there exists an effectively computable absolute constant c_7 such that every conjugacy class of $\text{Gal}(E/K)$ is represented by a Frobenius element of a prime ideal $v \in \Sigma_K$ which is unramified in E , such that*

$$\text{Nm}_{K/\mathbb{Q}}(v) \leq c_7 \cdot (\log \Delta_E + n_E \log N)^2.$$

Moreover, we can take v to be of degree 1, unramified in K/\mathbb{Q} , and not divide N .

Proof. This is proven in [18] for $K = \mathbb{Q}$. Thanks to Bach's improvement to the effective Chebotarev theorem (that we can take v to be unramified in K/\mathbb{Q}), the same argument works for arbitrary number fields. For completeness, we recall the proof below.

Clearly, we can assume that N is squarefree. Define $E' = E[\sqrt{N}]$. Then every prime of E' lying over a prime divisor of N is ramified in E'/\mathbb{Q} .

Now, we apply effective Chebotarev to $\text{Gal}(E'/K)$, to conclude that every conjugacy class of $\text{Gal}(E'/K)$ is represented by a Frobenius element of a prime ideal $v \in \Sigma_K$ of degree 1 which is unramified in E' and in K/\mathbb{Q} , and thus is coprime to N , such that $\text{Nm}_{\mathbb{Q}}^K(v) \leq c_5(\log \Delta_{E'})^2$. Since E'/E is ramified only at primes dividing $2N$, we can bound $\Delta_{E'}$ using Proposition 5 of section 1.3 of [18], and thereby conclude we can take v so that

$$\begin{aligned} \text{Nm}_{\mathbb{Q}}^K(v) &\leq c_5(\log \Delta_{E'})^2 \\ &\leq c_5 \cdot (2 \log \Delta_E + n_E \log 2N + n_E \log 2)^2 \\ &\leq c_7 \cdot (\log \Delta_E + n_E \log N)^2 \end{aligned}$$

for some effectively computable absolute constant c_7 . \square

6.3 Proof of Theorem 6.4

Theorem 6.4. *Let K be a number field. Then, there exists a finite set S_K of prime numbers depending only on K such that, for a prime $\ell \notin S_K$, and an elliptic curve E over K for which $E[\ell] \otimes \overline{\mathbb{F}}_\ell$ is reducible with degree 1 associated character ψ , one of the following holds.*

1. *There exists a CM elliptic curve E' , which is defined over K and whose CM-field is contained in K , with an ℓ -adic degree 1 associated character whose mod- ℓ reduction ψ' satisfies:*

$$\psi^{12} = (\psi')^{12}$$

2. *The Generalized Riemann Hypothesis fails for $K[\sqrt{-\ell}]$, and*

$$\psi^{12} = \text{cyc}_\ell^6,$$

where cyc_ℓ is the cyclotomic character. (Moreover, in this case we must have $\ell \equiv 3 \pmod{4}$ and the representation $\rho_{E,\ell}$ is already reducible over \mathbb{F}_ℓ .)

Proof. Since $\rho_{E,\ell}$ is reducible and 2-dimensional, its semisimplification is the direct sum of two associated characters ψ_1 and ψ_2 . If $\psi_1^{12} \notin \{1, \text{cyc}_\ell^6, \text{cyc}_\ell^{12}\}$, then by Lemma 6.1, Case 1 holds. Hence, it remains to show that Case 2 holds when $\psi_1^{12} \in \{1, \text{cyc}_\ell^6, \text{cyc}_\ell^{12}\}$.

Case 1: $\psi_1^{12} \in \{1, \text{cyc}_\ell^{12}\}$. If $\psi_1^{12} = \text{cyc}_\ell^{12}$, then the Weil pairing gives

$$\psi_2^{12} = (\text{cyc}_\ell \otimes \psi_1^{-1})^{12} = \text{cyc}_\ell^{12} \otimes (\psi_1^{12})^{-1} = 1.$$

Thus, by interchanging indices if necessary, we can assume without loss of generality that ψ_1^{12} is trivial.

Then, ψ_1 defines a degree (at most) 12 extension M of K . By construction, the Galois group $\text{Gal}(K^{\text{ab}}/M)$ is killed by ψ_1 , so when we consider E as a curve over M , the character ψ_1 is trivial. Thus, we have a Galois-invariant subspace $V \subset E[\ell]$ such that either V is pointwise fixed by $G_M = \text{Gal}(\overline{K}/M)$, or the quotient $E[\ell]/V$ is pointwise fixed by G_M . In the first case, E has an ℓ -torsion point defined over M , and in the second case, the isogenous curve E/V has an ℓ -torsion point defined over M . Writing $n_M \leq 12n_K$ for the degree of M , Merel's Theorem [10] implies that

$$\ell \leq \left(\sqrt{3^{n_M}} + 1 \right)^2 \leq \left(3^{6n_K} + 1 \right)^2.$$

Thus, so long as we choose S_K to contain all primes at most $\left(3^{6n_K} + 1 \right)^2$, we are done.

Case 3: $\psi_1^{12} = \text{cyc}_\ell^6$. The Weil pairing implies

$$\psi_2^{12} = (\text{cyc}_\ell \otimes \psi_1^{-1})^{12} = \text{cyc}_\ell^{12} \otimes (\psi_1^{12})^{-1} = \text{cyc}_\ell^{12} \otimes (\text{cyc}_\ell^6)^{-1} = \text{cyc}_\ell^6.$$

In other words,

$$\tilde{\rho}_{E,\ell}^{12} = \text{cyc}_\ell^6 \oplus \text{cyc}_\ell^6.$$

If $\rho_{E,\ell}$ is irreducible over \mathbb{F}_ℓ , then $\tilde{\rho}_{E,\ell} = \rho_{E,\ell}$, so the projective image of $\rho_{E,\ell}$ in $\text{PGL}_2(\mathbb{F}_\ell)$ has order at most 6. But by Lemma 18' of [18] (which is stated for $K = \mathbb{Q}$, but the same proof works as long as ℓ is unramified in K), the projective image has an element of order at least $(\ell - 1)/4$. Hence, as long as we choose S_K to contain all primes less than 25, it follows that $\rho_{E,\ell}$ is already reducible over \mathbb{F}_ℓ .

In particular, cyc_ℓ^6 is the 12th power of some character valued in \mathbb{F}_ℓ^\times . Since we are assuming ℓ is unramified in K , the cyclotomic character surjects onto \mathbb{F}_ℓ^\times . Thus, every 12th power in \mathbb{F}_ℓ^\times is a 6th power, so $\ell \equiv 3 \pmod{4}$.

Now, suppose GRH holds for $K[\sqrt{-\ell}]$. Then, by Corollary 6.3, we could find a prime ideal v of K such that v is split in $K[\sqrt{-\ell}]$, of degree 1, does not lie over 3, and satisfies the inequality

$$\begin{aligned} \text{Nm}_{\mathbb{Q}}^K(v) &\leq c_7 \cdot (\log \Delta_{K[\sqrt{\pm\ell}]} + n_{K[\sqrt{\pm\ell}]} \log 3)^2 \\ &= 4c_7 \cdot (2 \log \Delta_K + 2n_K \log 3 + n_K \log \ell)^2. \end{aligned}$$

We claim that $\psi_1(\pi_v) + \psi_2(\pi_v) = 0$, for any ℓ more than some constant depending on K alone. Indeed we have

$$\psi_1(\pi_v) + \psi_2(\pi_v) \equiv \sqrt{\text{Nm}_{\mathbb{Q}}^K(v)} \cdot (\zeta + \bar{\zeta}) \pmod{\mathfrak{l}}$$

for some 12th root of unity ζ . Since v does not lie over 3, the right-hand side cannot be a nonzero rational number. Thus, if $\psi_1(\pi_v) + \psi_2(\pi_v) \neq 0$, we have a nontrivial divisibility condition on ℓ :

$$\ell \left| \text{Nm}_{\mathbb{Q}}^{\mathbb{Q}[\sqrt{\text{Nm}_{\mathbb{Q}}^K(v) \cdot (\zeta + \bar{\zeta})}]} \left(\sqrt{\text{Nm}_{\mathbb{Q}}^K(v)} \cdot (\zeta + \bar{\zeta}) - (\psi_1(\pi_v) + \psi_2(\pi_v)) \right) \right|.$$

But under any complex embedding, we have

$$\left| \sqrt{\text{Nm}_{\mathbb{Q}}^K(v)} \cdot (\zeta + \bar{\zeta}) - (\psi_1(\pi_v) + \psi_2(\pi_v)) \right| \leq \left(1 + \sqrt{\text{Nm}_{\mathbb{Q}}^K(v)} \right)^2.$$

Since $\mathbb{Q}[\sqrt{\text{Nm}_{\mathbb{Q}}^K(v) \cdot (\zeta + \bar{\zeta})}]$ is a quadratic field, we have

$$\ell \leq \left(1 + \sqrt{\text{Nm}_{\mathbb{Q}}^K(v)} \right)^4 \leq (1 + 2\sqrt{c_7} \cdot (2 \log \Delta_K + 2n_K \log 3 + n_K \log \ell))^4.$$

But this is clearly impossible for all ℓ larger than a constant depending on K alone. Thus, we have $\psi_1(\pi_v) + \psi_2(\pi_v) = 0$. Hence,

$$(\psi_1(\pi_v) - \psi_2(\pi_v))^2 = (\psi_1(\pi_v) + \psi_2(\pi_v))^2 - 4\psi_1(\pi_v)\psi_2(\pi_v) = -4\text{Nm}_{\mathbb{Q}}^K v,$$

which is a quadratic nonresidue mod ℓ , contradicting the reducibility of $\rho_{E,\ell}$. \square

Corollary 6.5. *Under GRH, the degrees of prime degree isogenies of elliptic curves over K are bounded uniformly if and only if K does not contain the Hilbert class field of an imaginary quadratic field F (i.e. if and only if there are no elliptic curves with CM defined over K).*

Proof. If K does not contain the Hilbert class field of an imaginary quadratic field F , then there are no CM elliptic curves which are defined over K and whose CM-field is contained in K . Thus, for $\ell \notin S_K$, we have that $\rho_{E,\ell}$ is absolutely irreducible for any elliptic curve E defined over K . In particular, E cannot admit an isogeny of degree ℓ .

Conversely, if K contains the Hilbert class field of an imaginary quadratic field F , then there is a CM elliptic curve defined over K , whose CM-field is contained in K . But such a curve has an isogeny of degree ℓ for all primes ℓ split in F . \square

7 Effective Results

In this section, we prove Theorem 7.9, which makes Theorems 5.16 and 6.4 (as well as Corollary 6.5) effective. The method of proof does not depend essentially on GRH; we only use GRH in Subsection 7.4 when putting everything together to get the final bound.

7.1 The Quantity c_g

Lemma 7.1. *Suppose n is a positive integer and $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] \leq 2g$. Then $n \mid c_g$.*

Proof. It suffices to prove this Lemma in the case where $n = q^k$ is a prime power. For every prime $p \neq q$, we have a natural symplectic form on $\mathcal{O}_{\mathbb{Q}[\zeta_n]}/(p)$ defined by

$$(\alpha, \beta) \mapsto \text{Tr}_{\mathbb{Q}}^{\mathbb{Q}[\zeta_n]} (\alpha\bar{\beta} - \beta\bar{\alpha}).$$

Multiplication by ζ_n thus defines an element of $\text{Sp}_{[\mathbb{Q}[\zeta_n] : \mathbb{Q}]}(\mathbb{F}_p)$ of order n for all odd primes $p \neq q$. Since we have an injection $\text{Sp}_{[\mathbb{Q}[\zeta_n] : \mathbb{Q}]}(\mathbb{F}_p) \hookrightarrow \text{Sp}_{2g}(\mathbb{F}_p)$, it follows that $n \mid c_g$ by the definition of c_g . \square

Theorem 7.2. *We have an explicit formula*

$$c_g = \prod_{\substack{\text{prime powers } p^n \\ (p-1)p^{n-1} \leq 2g < (p-1)p^n}} p^n.$$

In particular, $c_1 = 12$. In general, c_g can be bounded by an exponential in g ,

$$c_g \leq c_1 \cdot (7.4)^g \leq c_1 \cdot 8^g$$

for an effectively computable absolute constant c_1 .

Proof. From the prime number theorem, we have

$$\prod_{\substack{\text{prime powers } p^n \\ (p-1)p^{n-1} \leq 2g < (p-1)p^n}} p^n = e^{2g(1+o(1))} \leq c_1 \cdot 7.4^g \leq c_1 \cdot 8^g$$

for some effectively computable absolute constant c_1 . Thus, it suffices to verify the formula for c_g . From Lemma 7.1, it is clear that c_g is divisible by the above product. To see the reverse implication, we need to show that every prime power p^n dividing c_g divides the above product.

Case 1: p is odd. By Dirichlet's Theorem, we can find an odd prime $q \neq p$ whose class modulo p^n generates the cyclic group $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Now, suppose there is an element $X \in \mathrm{Sp}_{2g}(\mathbb{F}_q)$ of order p^n . By applying the Frobenius automorphism of $\overline{\mathbb{F}}_q$ to X , we see that if X has an eigenvalue ω , then it must also have an eigenvalue ω^q . Therefore, every primitive (p^n) th root of unity is an eigenvalue of X . It follows that $(p-1)p^{n-1} = |(\mathbb{Z}/p^n\mathbb{Z})^\times| \leq 2g$, which completes the proof.

Case 2: $p = 2$. By Dirichlet's Theorem, we can find an odd prime $q \equiv 3 \pmod{2^n}$. Now, suppose there is an element $X \in \mathrm{Sp}_{2g}(\mathbb{F}_q)$ of order 2^n . By applying the Frobenius automorphism of $\overline{\mathbb{F}}_q$ to X , we see that if X has an eigenvalue ω , then it must also have an eigenvalue ω^q . Since $X \in \mathrm{Sp}_{2g}(\mathbb{F}_q)$, we see that if X has an eigenvalue ω , it must also have an eigenvalue ω^{-1} .

But it is a standard fact from elementary number theory that $q \equiv 3$ and -1 generate the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Since X has order 2^n , it has some eigenvalue which is a primitive (2^n) th root of unity; therefore, every primitive (2^n) th root of unity is an eigenvalue of X . It follows that $2^{n-1} = |(\mathbb{Z}/2^n\mathbb{Z})^\times| \leq 2g$, which completes the proof. \square

7.2 Balanced Characters

In this subsection, we make Lemma 5.6 effective; we also note that balanced characters have a useful condition on their archimedean valuations, which will be helpful for making other arguments effective.

Lemma 7.3. *When θ^S is balanced with $S(\sigma) + S(\tau) = a'$, then for any archimedean absolute value $|\cdot|$ on K , we have*

$$|\theta^S(x)| = \sqrt{\mathrm{Nm}_{\mathbb{Q}}^K(x)}^{a'}.$$

Proof. Clear from Definition 2.14. \square

There is only a finite set of ℓ that can possibly be associated to a unbalanced character for some abelian variety. In what follows we will quantify this possible unbalanced set. For every unbalanced character θ^S , there exists some unit u_S for which $\theta^S(u_S)$ is not a root of unity. Now, observe that we have a natural action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the elements S of $\mathbb{Z}[\Gamma_K]$. If S and S' are related under this action, then $\theta^S(u)$ is Galois-conjugate to $\theta^{S'}(u)$; in particular, $\theta^S(u)$ is a root of unity if and only if $\theta^{S'}(u)$ is a root of unity. This implies that we can choose the u_S so they depend only on the orbit of S under the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If we do this, then

$$B_{\text{char}}(K, g) := \prod_{\theta^S \text{ unbalanced}} \left(1 - \theta^S(u_S)^{c_g/e}\right)$$

is a rational integer. Moreover, by Definition 5.3, any prime ℓ for which a corresponding character θ^S is unbalanced must divide $B_{\text{char}}(K, g)$.

Lemma 7.4. *There exists an effectively computable absolute constant c_8 such that we can choose the u_S so that the following inequality holds:*

$$B_{\text{char}}(K, g) \leq c_8 \cdot \exp \left(\frac{2 \cdot R_K \cdot (r_K + 2)! \cdot (2g \cdot c_g + 1)^{n_K+1} \cdot (\log n_K)^3}{|\log \log n_K|^3} \right).$$

Remark 7.5. The constant $B_{\text{char}}(K, g)$ can be effectively directly computed for any field K , and in many interesting cases (such as quadratic imaginary fields) is small.

Proof. Define the multiplicative Minkowski embedding μ and functions f^S as in the proof of Lemma 2.15. Suppose that θ^S is a unbalanced character.

Write $\Lambda_S \subset \Lambda$ for the kernel of f^S . Since θ^S is unbalanced, it follows that $\Lambda_S \subsetneq \Lambda$. Observe that by definition, f^S does not vanish on any element of the quotient lattice Λ/Λ_S . Therefore, to choose u_S so that $f^S(u_S)$ is small, it suffices to find a short lattice vector of the quotient lattice Λ/Λ_S , which we can do via Minkowski's Theorem if we first bound

$$\text{vol}(\Lambda/\Lambda_S) = \frac{\text{vol}(\Lambda)}{\text{vol}(\Lambda_S)} = \frac{R_K \sqrt{r_K + 1}}{\text{vol}(\Lambda_S)}.$$

(Here, we think about Λ/Λ_S sitting inside the real vector space $\mathbb{R}_0^{r_K+1}/\langle \Lambda_S \rangle$. We give $\mathbb{R}_0^{r_K+1}/\langle \Lambda_S \rangle$ an inner product by identifying it with the orthogonal complement of Λ_S and taking the induced inner product from $\mathbb{R}_0^{r_K+1}$.) To do this, we use the following theorem of Voutier:

Theorem (Voutier [20]). *For any $u \in \mathcal{O}_K^\times$ which is not a root of unity, we have the inequality*

$$\log \left(\prod_{i=1}^{n_K} \max(1, |\sigma_i(u)|) \right) \geq \alpha \quad \text{where} \quad \alpha = \frac{1}{4} \left(\frac{\log \log n_K}{\log n_K} \right)^3.$$

It follows that the length of any unit in Λ under the L^1 norm (i.e. the sum of the absolute values of the coordinates) satisfies

$$\|\mu(u)\|_{L^1} = \sum_{i=1}^{r_1} |\log |\sigma_i(u)|| + \sum_{i=r_1+1}^{r_1+r_2} 2|\log |\sigma_i(u)|| = 2 \cdot \log \left(\prod_{i=1}^{n_K} \max(1, |\sigma_i(u)|) \right) \geq 2\alpha.$$

(For the second equality above, we have used $\sum_{i=1}^{n_K} \log |\sigma_i(u)| = 0$.) Now, extend the lattice Λ_S to a lattice Λ'_S of dimension $r_K + 1$ by adding more basis vectors which are mutually orthogonal, orthogonal to Λ_S , and whose length (under the Euclidean metric) equals 2α . From the above Theorem, the (open) unit L^1 -ball of radius 2α intersects the lattice Λ'_S only at the origin. Therefore, by Minkowski's Theorem,

$$\text{vol}(\Lambda'_S) \geq \frac{1}{2^{r_K+1}} \cdot \left(\frac{2^{r_K+1}}{(r_K+1)!} \cdot (2\alpha)^{r_K+1} \right) = \frac{(2\alpha)^{r_K+1}}{(r_K+1)!}.$$

Now, write c for the codimension of Λ_S in Λ . Then, we have

$$\text{vol}(\Lambda_S) = \frac{1}{(2\alpha)^{c+1}} \cdot \text{vol}(\Lambda'_S) \geq \frac{1}{(2\alpha)^{c+1}} \cdot \frac{(2\alpha)^{r_K+1}}{(r_K+1)!} = \frac{(2\alpha)^{r_K-c}}{(r_K+1)!}$$

which gives

$$\text{vol}(\Lambda/\Lambda_S) = \frac{\text{vol}(\Lambda)}{\text{vol}(\Lambda_S)} \leq \frac{R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)!}{(2\alpha)^{r_K-c}}.$$

Applying Minkowski's Theorem again, we can find some vector of Λ/Λ_S whose length under the Euclidean metric (we use the Euclidean metric because the L^1 metric on \mathbb{R}^{r_K+1} does not induce the L^1 metric on $\mathbb{R}_0^{r_K+1}/\langle \Lambda_S \rangle$) is bounded by (here, we use that the volume of the unit Euclidean c -ball is greater than that of the unit L^1 -ball, $2^c/c!$)

$$\begin{aligned} (\text{vol}(\Lambda/\Lambda_S) \cdot c!)^{\frac{1}{c}} &\leq \left(\frac{R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)!}{(2\alpha)^c} \cdot c! \right)^{\frac{1}{c}} \\ &= \frac{1}{2\alpha} \cdot (R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)! \cdot c!)^{\frac{1}{c}} \end{aligned}$$

The above function is a decreasing function of c , since $R_K \geq 1/5$ by [5]. Thus,

$$\leq \frac{R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)!}{2\alpha}.$$

Thus, we can find some vector of Λ/Λ_S whose length under the metric induced from the L^1 metric on \mathbb{R}^{r_K+1} is bounded by

$$\sqrt{r_K+1} \cdot \frac{R_K \cdot \sqrt{r_K+1} \cdot (r_K+1)!}{2\alpha} \leq \frac{R_K \cdot (r_K+2)!}{2\alpha}.$$

Now, observe that $|f^S(u)| \leq 2g \cdot c_g \cdot \|\mu(u)\|_{L^1}$ for any S . Therefore, for any unbalanced character θ^S , we can select u_S such that $\theta^S(u_S)$ is not a root of unity, and

$$|\log |\theta^{S'}(u_S)^{c_g/e}|| \leq M \quad \text{where} \quad M := 2g \cdot c_g \cdot \frac{R_K \cdot (r_K + 2)!}{2\alpha}$$

where S' is any subset of Γ_K . This gives

$$\begin{aligned} B_{\text{char}}(K, g) &= \prod_{\substack{S \subset \Gamma_K \\ \theta^S \text{ is unbalanced}}} (1 - \theta^S(u_S)^{c_g/e}) \\ &\leq \prod_{\substack{S \subset \Gamma_K \\ \theta^S \text{ is unbalanced}}} (1 + |\theta^S(u_S)^{c_g/e}|) \\ &\leq (1 + \exp(M))^{(2g \cdot c_g + 1)^{n_K}}. \end{aligned}$$

Since $\exp(M) \geq c_9 \cdot (2g \cdot c_g + 1)^{n_K}$ for some effectively computable absolute constant c_9 , we have for some effectively computable absolute constant c_8 ,

$$\begin{aligned} B_{\text{char}}(K, g) &\leq c_8 \cdot \exp(M \cdot (2g \cdot c_g + 1)^{n_K}) \\ &= c_8 \cdot \exp\left(\frac{2 \cdot R_K \cdot (r_K + 2)! \cdot (2g \cdot c_g + 1)^{n_K + 1} \cdot (\log n_K)^3}{(\log \log n_K)^3}\right). \quad \square \end{aligned}$$

For the remainder of this paper, we suppose that $\ell \nmid B_{\text{char}}(K, g)$; in particular, this implies that θ^S is a balanced character.

7.3 Bounds for Theorem 5.15

We begin this section by bounding the number of possible values of $\psi_{\mathbb{C}}(v)$.

Lemma 7.6. *Let $v \subset \mathcal{O}_K$ be a prime ideal, with $\text{Nm}_{\mathbb{Q}}^K v \leq V$. Then, as A ranges over all abelian varieties of dimension g , d ranges over all integers between 0 and $2g$, and ℓ ranges over all rational primes coprime to x , there are at most*

$$B_{\text{poss}}(K, g, V) = c_{10} \cdot (256 \cdot V)^{\frac{g(g+1)}{4}}$$

possible values of $\psi_{\mathbb{C}}(v)$, for some effectively computable absolute constant c_{10} . Moreover, the magnitude of $\psi_{\mathbb{C}}(v)$ under any complex embedding is bounded by V^g .

Proof. First, we count the number of possible polynomials P_{π} satisfying Lemma 4.1, assuming that all of its roots have magnitude equal to the square root of the norm of v , under any complex embedding. The first $g + 1$ coefficients of P_{π} determine the rest, since the roots of P_{π} come in pairs which multiply to the norm of v . Thus, to find the total number

of possible such polynomials, we can multiply together the number of possible values for the coefficient of z^{2g-i} in P_π for $0 \leq i \leq g$. This gives

$$\begin{aligned} \prod_{0 \leq i \leq g} \left(2 \cdot \binom{2g}{i} \cdot \left(\sqrt{\text{Nm}_{\mathbb{Q}}^K(x)} \right)^i \right) &= 2^{g+1} \cdot (\text{Nm}_{\mathbb{Q}}^K(x))^{\frac{g(g+1)}{4}} \cdot \prod_{0 \leq i \leq 3} \binom{2g}{i} \cdot \prod_{4 \leq i \leq g} \binom{2g}{i} \\ &\leq 2^{g+1} \cdot (\text{Nm}_{\mathbb{Q}}^K(x))^{\frac{g(g+1)}{4}} \cdot \prod_{0 \leq i \leq 3} \binom{2g}{i} \cdot (2^{2g})^{g-3} \\ &\leq \frac{c_{11}}{64^g} \cdot (256 \cdot \text{Nm}_{\mathbb{Q}}^K(x))^{\frac{g(g+1)}{4}} \end{aligned}$$

for some effectively computable absolute constant c_{11} .

Now, any value of $\psi_{\mathbb{C}}(v)$ can be written as a product of distinct roots of such a polynomial, times a c_g th root of unity, times a power of $\text{Nm}_{\mathbb{Q}}^K v$ which is at most g . Therefore, the number of possible values of $\psi_{\mathbb{C}}(v)$ is at most the product of the number of possible polynomials calculated above and $2^{2g} \cdot c_g \cdot (g+1) \leq c_1 \cdot 64^g$. This implies the statement of this lemma. \square

Let us fix a direct sum decomposition

$$\text{Cl}(K) \simeq \mathbb{Z}/h'_K \mathbb{Z} \oplus H(K),$$

for a subgroup $H(K) \subset \text{Cl}(K)$, and fix a generator α of $\mathbb{Z}/h'_K \mathbb{Z}$. From elementary group theory, the image of any homomorphism from $\text{Cl}(K)$ to a cyclic group is generated by the image of some element in $\alpha + H(K)$.

Choose prime ideals $\{v_1, v_2, \dots, v_{h_K/h'_K}\}$ which are of degree 1, coprime to $c_g \cdot h_K$, and represent each element of $\alpha + H(K)$. Also, write $(v_i)^{h'_K} = (x_i)$.

In order to make Theorem 5.15 effective, we note that if ψ is an associated character which does not satisfy the conclusion of Theorem 5.15, then our proof shows that either θ^S is unbalanced, or there is some i so that Lemma 5.8 fails for v_i . Thus the quantity $B_{\text{rat}}(K, g)$, which we define to be the product of

$$\prod_{\text{balanced characters } \theta^S} \left(\prod_{i=1}^{h_K/h'_K} \prod_{\substack{\text{possible values of } \psi(\pi_{v_i}) \\ \psi(\pi_{v_i})^{c_g \cdot h'_K} \neq \theta^S(x_i)^{c_g/e}}} \left(\psi(\pi_{v_i})^{c_g \cdot h'_K} - \theta^S(x_i)^{c_g/e} \right) \right)$$

with all primes which lie under one of the v_i or divide Δ_K , is a rational integer with the property that we can take $S_{K,g}$ to consist of all primes dividing $B_{\text{rat}}(K, g) \cdot B_{\text{char}}(K, g)$.

Lemma 7.7. *We have*

$$B_{\text{rat}}(K, g) \leq \left(2 \cdot V^{2g \cdot c_g \cdot h'_K} \right)^{\sqrt{(2g \cdot c_g + 1)^{n_K} \cdot (h_K/h'_K) \cdot B_{\text{poss}}(K, g, V)}} \cdot V^{h_K/h'_K} \cdot \Delta_K,$$

where V is the maximum norm of the v_i .

Proof. Under any complex embedding, Lemma 7.3 implies that

$$\begin{aligned} \left| \psi(\pi_{v_i})^{c_g \cdot h'_K} - \theta^S(x_i)^{c_g/e} \right| &\leq \left| \psi(\pi_{v_i})^{c_g \cdot h'_K} \right| + \left| \theta^S(x_i)^{c_g/e} \right| \\ &\leq 2 \cdot |\mathrm{Nm}_{\mathbb{Q}}^K v_i|^{2g \cdot c_g \cdot h'_K} \\ &\leq 2 \cdot V^{2g \cdot c_g \cdot h'_K} \end{aligned}$$

which completes the proof, using Lemma 7.6, together with the fact that there at most $\sqrt{(2g \cdot c_g + 1)^{n_K}}$ balanced characters. (The factor of V^{h_K/h'_K} is there to account for the primes which lie under one of the v_i .) \square

7.4 Proof of Theorem 7.9

In this subsection, we prove Theorem 7.9. While Theorem 5.16 is true unconditionally, assuming GRH allows us to get a significantly better bound.

Remark 7.8. Using an unconditional version of the Chebotarev Density Theorem (see Remark 6.2), one could make Theorem 7.9 unconditional using the same method. In the case of $g = 1$, there is also an unconditional bound due to David; see Theorem 2 of [2]. (The logarithm of David's bound is roughly the n_K th power of the logarithm of the conditional bound given here.)

Theorem 7.9. *Under GRH, there are effectively computable absolute constants c_2 , c_3 , and c_4 such that we can take in Theorems 6.4 and 5.16*

$$\begin{aligned} \prod_{\ell \in S_K} \ell &\leq \exp \left(c_2^{n_K} \cdot (R_K \cdot n_K^{r_K} + h_K^2 \cdot (\log \Delta_K)^2) \right) \\ \prod_{\ell \in S_{K,g}} \ell &\leq \exp \left(c_3^{n_K} \cdot \left(8^{g(n_K+1)} \cdot R_K \cdot n_K^{r_K} + 3^{g \cdot n_K} \cdot (c_4 \cdot g \cdot h_K \cdot n_K \cdot \log \Delta_K)^{\frac{g(g+1)}{2}+1} \right) \right). \end{aligned}$$

Remark 7.10. In fact, we have proven (independently of GRH) that

$$\prod_{\ell \in S_{K,g}} \ell \leq B_{\mathrm{char}}(K, g) \cdot B_{\mathrm{rat}}(K, g).$$

Proof. Under GRH, Corollary 6.3 (applied to $N = c_g \cdot h_K$), and $\log h_K \leq \frac{3}{2} \log \Delta_K$ (which follows from [8], Theorem 6.5), implies that we can choose the v_i so that

$$V = \max \mathrm{Nm}_{\mathbb{Q}}^K(v_i) \leq c_7 \cdot (\log \Delta_{H_K} + n_{H_K} \log(c_g \cdot h_K))^2 \leq c_{12} \cdot g^2 \cdot h_K^2 \cdot n_K^2 \cdot (\log \Delta_K)^2$$

for some effectively computable absolute constant c_{12} .

We use the notation $f \lesssim g$ to mean that $f \leq C \cdot g$ for an effectively computable absolute constant C .

By Remark 7.10 above, it suffices to show both of $\log B_{\text{char}}(K, g)$ and $\log B_{\text{rat}}(K, g)$ are bounded by a constant times the logarithm of the right-hand side of the first inequality appearing in the statement of the theorem. First, we bound $B_{\text{char}}(K, g)$, as follows.

$$\log B_{\text{char}}(K, g) \lesssim \frac{R_K \cdot (r_K + 2)! \cdot (2g \cdot c_g + 1)^{n_K + 1} \cdot (\log n_K)^3}{|\log \log n_K|^3} \lesssim 8^{g(n_K + 1)} \cdot R_K \cdot (c_3 n_K)^{r_K}$$

for some effectively computable absolute constant c_3 . Next, we bound $B_{\text{rat}}(K, g)$, using $\log h_K \leq \frac{3}{2} \log \Delta_K$:

$$\begin{aligned} \log B_{\text{rat}}(K, g) &\lesssim g \cdot c_g \cdot h'_K \cdot \sqrt{(2g \cdot c_g + 1)^{n_K} \cdot (\log g + \log h_K + \log n_K + \log \log \Delta_K)} \\ &\quad \cdot (h_K / h'_K) \cdot (256 \cdot c_{12} \cdot g^2 \cdot h_K^2 \cdot n_K^2 \cdot (\log \Delta_K)^2)^{\frac{g(g+1)}{4}} \\ &\lesssim (c_{13} \cdot 3^g)^{n_K} \cdot (c_4 \cdot g \cdot h_K \cdot n_K \cdot \log \Delta_K)^{\frac{g(g+1)}{2} + 1} \end{aligned}$$

for effectively computable absolute constants c_4 and c_{13} .

Now, from the proof of Theorem 6.4, it suffices to show that the logarithm of the product of all primes ℓ for which

$$\ell \leq (3^{12n_K} + 1)^2 \quad \text{or} \quad \ell \leq (1 + 2\sqrt{c_7} \cdot (2 \log \Delta_K + 2n_K \log 3 + n_K \log \ell))^8$$

is bounded by an absolute constant times the logarithm of the right-hand side of the second inequality appearing in the statement of the theorem. For the product of all primes satisfying the first of the above two inequalities, this is clear from the prime number theorem.

For the second factor, note that the Brauer-Siegel theorem (which is effective under GRH) implies that

$$c_2^{n_K} \cdot (R_K \cdot n_K^{r_K} + h_K^2 \cdot (\log \Delta_K)^4) \gtrsim h_K^2 + n_K^{n_K/2} \cdot R_K \gtrsim n_K^{n_K/3} \cdot (h_K R_K)^{2/3} \gtrsim \Delta_K^{1/4}.$$

Thus, it suffices to show that for $\ell \geq \sqrt[4]{\Delta_K}$ and more than an effectively computable absolute constant, we have

$$\ell \geq (1 + 2\sqrt{c_7} \cdot (2 \log \Delta_K + 2n_K \log 3 + n_K \log \ell))^4.$$

But this is clear, since Minkowski's bound together with the assumption that $\ell \geq \sqrt[4]{\Delta_K}$ imply that the right-hand side of the above inequality is at most an effectively computable absolute constant times $(\log \ell)^8$. This completes the proof. \square

References

- [1] Eric Bach and Jonathan Sorenson. Explicit bounds for primes in residue classes. *Math. Comp.*, 65(216):1717–1735, 1996.

- [2] Agnès David. Caractère d'isogénie et critères d'irréductibilité. Preprint available online at <http://arxiv.org/abs/1103.3892>.
- [3] Pierre Deligne. Travaux de Shimura. In *Séminaire Bourbaki, 23ème année (1970/71)*, Exp. No. 389, pages 123–165. Lecture Notes in Math., Vol. 244. Springer, Berlin, 1971.
- [4] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.
- [5] Eduardo Friedman. Analytic formulas for the regulator of a number field. *Invent. Math.*, 98(3):599–622, 1989.
- [6] Alexander Grothendieck. Modèles de Néron et monodromie. In *Séminaire de Géométrie Algébrique, Volume 7, Exposé 9*.
- [7] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.
- [8] H. W. Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992.
- [9] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.
- [10] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.
- [11] J. S. Milne. Abelian varieties defined over their fields of moduli. I. *Bull. London Math. Soc.*, 4:370–372, 1972.
- [12] J.S. Milne. Complex multiplication (v0.00), 2006. Available at www.jmilne.org/math/.
- [13] Fumiyuki Momose. Isogenies of prime degree over number fields. *Compositio Math.*, 97(3):329–348, 1995.
- [14] Michel Raynaud. Schémas en groupes de type (p, \dots, p) . *Bull. Soc. Math. France*, 102:241–280, 1974.
- [15] Jordan Rizov. Fields of definition of rational points on varieties. 2005. Available at <http://arxiv.org/abs/math/0505364>.
- [16] Jean-Pierre Serre. *Abelian l -adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

- [17] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
- [18] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.
- [19] Goro Shimura. Algebraic number fields and symplectic discontinuous groups. *Ann. of Math. (2)*, 86:503–592, 1967.
- [20] Paul Voutier. An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74(1):81–95, 1996.

A A Determinantal Comparison (by Brian Conrad)

A.1 Motivation

For a linear representation ρ of a group Γ on a finitely generated module $V = \prod V_i$ over a finite product $\prod F_i$ of fields F_i , we get a determinant $\det \rho: \Gamma \rightarrow \prod F_i^\times$ via the Γ -action on $\prod \det(V_i)$. (This is the usual $(\prod F_i)$ -linear determinant when V is free as a $(\prod F_i)$ -module.) The case of interest to us will be $\Gamma = G_K := \text{Gal}(K_s/K)$ for a finite extension K of \mathbb{Q}_p and the action of G_K on $V = V_p(A)$ for an abelian variety A of dimension $g > 0$ over K .

Consider a commutative subfield $F \subseteq \text{End}_K^0(A)$ (which could even be \mathbb{Q} , though that case will not be interesting), so for $F_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} F$, there is a natural continuous F_p -linear representation $\rho_{A,p}$ of G_K on $V_p(A)$. This yields a continuous determinant homomorphism $G_K^{\text{ab}} \rightarrow F_p^\times$. Composing with the Artin map $r_K: K^\times \rightarrow G_K^{\text{ab}}$, we get a composite map

$$\psi_A: K^\times \xrightarrow{r_K} G_K^{\text{ab}} \xrightarrow{\det_{F_p} \rho_{A,p}} F_p^\times.$$

A natural question, inspired by the use of the reflex norm in the Main Theorem of complex multiplication, is to ask whether the restriction of ψ_A to an open subgroup of \mathcal{O}_K^\times can be described in terms of the F -action on $\text{Lie}(A)$. To be precise, $\text{Lie}(A)$ is naturally a module over $K \otimes_{\mathbb{Q}} F = K \otimes_{\mathbb{Q}_p} F_p$, so K acts F_p -linearly on $\text{Lie}(A)$ and hence we can take the F_p -linear determinant of (the inverse of) the K^\times -action on $\text{Lie}(A)$:

$$\chi_A(a) = \det_{F_p}((x \mapsto a \cdot x): \text{Lie}(A) \rightarrow \text{Lie}(A)).$$

It is natural to ask if the homomorphisms $\psi_A, \chi_A: K^\times \rightrightarrows F_p^\times$ are equal on an open subgroup of \mathcal{O}_K^\times when F is a totally real or CM field. The answer is affirmative without archimedean restrictions on F , and by using p -adic Hodge theory in the form due to Fontaine (see [3], [4]), which goes beyond what was used by Serre and Tate (who worked in the area before the discovery of B_{crys}) we can say a bit more:

Theorem A.1. *The two maps $K^\times \rightrightarrows F_p^\times$ coincide on an open subgroup of \mathcal{O}_K^\times . If A has semistable reduction then these maps agree on \mathcal{O}_K^\times .*

Example 1. If A is a CM abelian variety with good reduction and F is a CM field with $[F : \mathbb{Q}] = 2g$ then this theorem recovers the inertial description of the reflex norm in the theory of complex multiplication when there is good reduction.

We will use Grothendieck’s orthogonality theorem in the semistable case to reduce Theorem A.1 to a more general assertion about p -divisible groups over the valuation ring of a finite extension of K . The main point is to then recast this general assertion in terms of p -adic Hodge theory, since that admits a robust tensorial structure whereas p -divisible groups do not. In what follows, we will use the covariant Fontaine functors (i.e., $(B \otimes_{\mathbb{Q}_p} V)^{G_K}$ rather than $\mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V, B)$).

A.2 Reformulation via p -divisible groups

To prove Theorem A.1, it is harmless to replace K with a finite extension so that A has semistable reduction. So we now assume this to be the case. Let \mathcal{A} denote the semi-abelian relative identity component of the Néron model $N(A)$ over \mathcal{O}_K (i.e., the open complement in $N(A)$ of the union of the non-identity components of the special fiber $N(A)_k$). The special fiber \mathcal{A}_k is an extension of an abelian variety B by a torus T . We will use a filtration on $V_p(A)$ arising from the filtration on \mathcal{A}_k to reduce our problem to an intrinsic question about p -divisible groups over \mathcal{O}_K .

Now we recall Grothendieck’s results on the structure of p -adic Tate modules of abelian varieties with semistable reduction over p -adic fields. (This is developed in [SGA 7, Exp. IX]; see [2, §4–§5] for an exposition, especially [2, Thm. 5.5].) Let $a = \dim B$ and $t = \dim T$. The “finite parts” of the $\mathcal{A}[p^n]$ (according to the decomposition of the quasi-finite flat separated \mathcal{O}_K -groups $\mathcal{A}[p^n]$ via Zariski’s Main Theorem) define a p -divisible group Γ over \mathcal{O}_K of height $2a + t$ lifting $\mathcal{A}_k[p^\infty]$. This has generic fiber contained in $A[p^\infty]$, and it is final among p -divisible groups over \mathcal{O}_K whose generic fiber is equipped with a map to $A[p^\infty]$. By Grothendieck’s orthogonality theorem, the quotient $V_p(A)/V_p(\Gamma)$ is the Galois representation associated to the Cartier dual of the unique p -divisible group Γ'_t over \mathcal{O}_K lifting the p -divisible group $T'[p^\infty]$ of the maximal torus T' in the special fiber of the Néron model of the dual abelian variety A' . Since Γ'_t has étale Cartier dual (as this holds for its special fiber $T'[p^\infty]$), it follows that $V_p(A)/V_p(\Gamma)$ is *unramified*. Hence, the inertial restriction of ψ_A is unaffected by replacing $V_p(A)$ with $V_p(\Gamma)$.

The Lie algebra of A is the generic fiber of $\mathrm{Lie}(\mathcal{A})$, and $\mathrm{Lie}(\mathcal{A})$ is naturally identified with the Lie algebra of the formal \mathcal{O}_K group $\widehat{\mathcal{A}} = \mathrm{Spf}(\mathcal{O}_{\mathcal{A},0}^\wedge)$ of \mathcal{A} (completion along the identity section over \mathcal{O}_K). But $\widehat{\mathcal{A}}$ is the formal group over \mathcal{O}_K corresponding to the connected part of the p -divisible group Γ under the Serre–Tate equivalence between connected p -divisible groups and commutative formal Lie groups on which $[p]$ is an isogeny (over any complete local noetherian ring with residue characteristic p). Hence, $\mathrm{Lie}(A) = \mathrm{Lie}(\Gamma)[1/p]$

functorially in the isogeny category over K . (Note that $\mathrm{Lie}(\Gamma)[1/p]$ is functorial with respect to K -homomorphisms in Γ , due to Tate's isogeny theorem for p -divisible groups over \mathcal{O}_K .) The F_p -action on $V_p(\Gamma)$ arises from an F_p -action on Γ in the isogeny category over \mathcal{O}_K .

We conclude that our entire problem is intrinsic to the p -divisible group Γ over \mathcal{O}_K , in the sense that it involves relating the inertial action on $\det_{F_p}(V_p(\Gamma))$ to the F_p -determinant of the K^\times -action on $\mathrm{Lie}(\Gamma)[1/p]$. In this way, our problem makes sense more generally for an arbitrary p -divisible group over \mathcal{O}_K equipped with an action by F_p in the isogeny category over \mathcal{O}_K . Decomposing Γ (up to isogeny over \mathcal{O}_K) according to the idempotents of F_p , and renaming each factor field of F_p as F , thereby reduces Theorem A.1 to:

Theorem A.2. *Let K be a finite extension of \mathbb{Q}_p , Γ a p -divisible group over \mathcal{O}_K , and F a finite extension of \mathbb{Q}_p equipped with an action on Γ in the isogeny category over \mathcal{O}_K .*

Let $\chi: K^\times \rightarrow F^\times$ be defined by the reciprocal of the F -linear determinant of the K^\times -action on $\mathrm{Lie}(\Gamma)[1/p]$, and let the composite map

$$\psi: K^\times \xrightarrow{r_K} G_K^{\mathrm{ab}} \longrightarrow F^\times$$

be defined by the F -linear determinant of the G_K -action on $V_p(\Gamma)$. Then $\psi|_{\mathcal{O}_K^\times} = \chi|_{\mathcal{O}_K^\times}$.

A.3 Proof of Theorem A.2

In view of how χ is constructed from a $(K \otimes_{\mathbb{Q}_p} F)$ -module, it arises from a homomorphism of \mathbb{Q}_p -tori $\mathrm{Res}_{\mathbb{Q}_p}^K \mathbb{G}_{m,K} \rightarrow \mathrm{Res}_{\mathbb{Q}_p}^F \mathbb{G}_{m,F}$. Thus, by [1, Prop. B.4(i)], $\chi|_{\mathcal{O}_K^\times}$ is the I_K -restriction of a crystalline representation $G_K^{\mathrm{ab}} \rightarrow F^\times$. Hence, if ψ and χ agree on an open subgroup of \mathcal{O}_K^\times then their ratio on \mathcal{O}_K^\times is the I_K -restriction of a crystalline representation that is finite on I_K . But a crystalline p -adic representation of G_K with finite image on I_K is unramified, so it would follow that χ and ψ coincide on \mathcal{O}_K^\times . In particular, if χ^e and ψ^e coincide on \mathcal{O}_K^\times for some $e > 0$ (so χ and ψ agree on the open subgroup $(\mathcal{O}_K^\times)^e$) then we will be done.

It is harmless to replace Γ with an \mathcal{O}_K -isogenous p -divisible group, so we may and do assume that \mathcal{O}_F acts on Γ (not just in the isogeny category). If F'/F is a finite extension then it is harmless to replace Γ with its power $\mathcal{O}_{F'} \otimes_{\mathcal{O}_F} \Gamma$ (defined in the evident manner), since at the determinant level we would be replacing χ and ψ with their $[F' : F]$ th powers, which we have seen is harmless. Thus, we may and do arrange that F splits K/\mathbb{Q}_p .

Let Γ^\vee denote the dual of Γ , and consider the \mathbb{C}_K -linear G_K -equivariant canonical Hodge–Tate decomposition $\mathbb{C}_K \otimes_{\mathbb{Q}_p} V_p(\Gamma) \simeq (\mathbb{C}_K(1) \otimes_K t_\Gamma) \oplus (\mathbb{C}_K \otimes_K \mathrm{Hom}_K(t_{\Gamma^\vee}, K))$, where $t_\Gamma := \mathrm{Lie}(\Gamma)[1/p]$ (and similarly for t_{Γ^\vee}). For later purposes, it will be convenient to apply the follow elementary lemma to rewrite the second summand.

Lemma A.3. *Let K and F be finite separable extensions of a field k . For any finitely generated $(K \otimes_k F)$ -module W , the $(K \otimes_k F)$ -modules $\mathrm{Hom}_K(W, K)$ and $\mathrm{Hom}_F(W, F)$ are naturally isomorphic, where F acts K -linearly on $\mathrm{Hom}_K(W, K)$ through functoriality applied to its K -linear action on W and similarly for the F -linear K -action on $\mathrm{Hom}_F(W, F)$.*

Proof. It suffices to prove that the natural $(K \otimes_k F)$ -linear map

$$\mathrm{Hom}_K(W, K) \rightarrow \mathrm{Hom}_k(W, k) \quad \text{defined via} \quad \ell \mapsto \mathrm{Tr}_k^K \circ \ell$$

is an isomorphism, as then we can argue similarly with the roles of K and F swapped. This only involves the underlying K -vector space of W (ignoring the F -action), so we can reduce to the trivial case $W = K$. \square

We now rewrite the Hodge–Tate decomposition in the form

$$\mathbb{C}_K \otimes_{\mathbb{Q}_p} V_p(\Gamma) \simeq (\mathbb{C}_K(1) \otimes_K t_\Gamma) \oplus (\mathbb{C}_K \otimes_K \mathrm{Hom}_F(t_{\Gamma^\vee}, F)), \quad (6)$$

where $\mathrm{Hom}_F(t_{\Gamma^\vee}, F)$ is a K -vector space through functorality applied to the F -linear K -action on t_{Γ^\vee} . Since F splits K/\mathbb{Q}_p , any $(K \otimes_{\mathbb{Q}_p} F)$ -module W (such as t_Γ and t_{Γ^\vee}) decomposes into F -subspaces

$$W = \bigoplus_\sigma W_\sigma$$

according to a \mathbb{Q}_p -embedding $\sigma: K \rightarrow F$ through which K acts. That is, for $w \in W_\sigma$ we have $(c \otimes 1)w = \sigma(c)w$ for $c \in K$. We can therefore compute the $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$ -linear determinant on both sides of (6) by first collapsing the K -action into the F -structure by decomposing modules into isotypic subspaces according to \mathbb{Q}_p -embeddings $\sigma: K \rightarrow F$, then decomposing those subspaces into isotypic \mathbb{C}_K -subspaces according to the \mathbb{Q}_p -embedding $F \rightarrow \mathbb{C}_K$ through which F acts, and then finally forming the \mathbb{C}_K -determinant of each such subspace of the latter sort. Thus, the $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$ -determinant of the left side of (6) is $\mathbb{C}_K \otimes_{\mathbb{Q}_p} \psi = \mathbb{C}_K \otimes_K (K \otimes_{\mathbb{Q}_p} \psi)$ and the $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$ -determinant of the right side of (6) is

$$\bigoplus_{\sigma: K \rightarrow F} \mathbb{C}_K \otimes_{K, \sigma} \left(\det_F(t_{\Gamma, \sigma}(1)) \otimes_F \det_F(\mathrm{Hom}_F(t_{\Gamma^\vee}, F)_\sigma) \right) \quad (7)$$

as σ varies through the \mathbb{Q}_p -embeddings of K into F .

Let $\theta_\chi: G_K^{\mathrm{ab}} \rightarrow \mathcal{O}_F^\times$ correspond to a map extending $\chi|_{\mathcal{O}_K^\times}$ via r_K , so it suffices to prove that ψ and θ_χ coincide on an open subgroup of \mathcal{O}_K^\times . It is equivalent to say that the ratio of these \mathcal{O}_F^\times -valued Hodge–Tate characters has finite image on inertia, or in other words that their \mathbb{C}_K -scalar extensions (over \mathbb{Q}_p) are $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$ -linearly and G_K -equivariantly isomorphic. In other words, it suffices to prove that $\mathbb{C}_K \otimes_{\mathbb{Q}_p} \theta_\chi$ is $(\mathbb{C}_K \otimes_{\mathbb{Q}_p} F)$ -linearly and G_K -equivariantly isomorphic to (7). It is harmless to replace G_K -equivariance with H -equivariance for an open subgroup H , such as the Galois group of \overline{K} over the Galois closure F' of F/\mathbb{Q}_p .

Our remaining task is to compute the Hodge–Tate weights of the \mathbb{C}_K -semilinear $G_{F'}$ -representation $\mathbb{C}_K \otimes_{j, F} \theta_\chi$ for each \mathbb{Q}_p -embedding $j: F \rightarrow \mathbb{C}_K$. For any such j the image $j(F)$ contains K and so induces a \mathbb{Q}_p -embedding of K into F . Since we use covariant Fontaine functors, the Hodge–Tate weight of $\mathbb{Q}_p(n)$ is $-n$ ($B_{\mathrm{HT}}(n)$ has its G_K -invariants occurring in degree $-n$). It therefore suffices to prove that for each \mathbb{Q}_p -embedding $\sigma: K \rightarrow F$,

the K -dimension of the σ -isotypic part of the $(K \otimes_{\mathbb{Q}_p} F)$ -module $\mathrm{gr}^n(D_{\mathrm{dR}}(\theta_\chi))$ vanishes for $n \neq n_\sigma := -\dim_F t_{\Gamma, \sigma}$ and is $[F : K]$ for $n = n_\sigma$. This means precisely that the σ -isotypic part of $D_{\mathrm{dR}}(\theta_\chi)$ is 1-dimensional over F with its unique nonzero gr^n occurring for $n = n_\sigma$.

Combining these assertions over all σ , our task is to prove that $D_{\mathrm{dR}}(\theta_\chi)$ is free of rank 1 over $K \otimes_{\mathbb{Q}_p} F$ and the σ -isotypic part of $\mathrm{gr}^\bullet(D_{\mathrm{dR}}(\theta_\chi))$ is supported in degree $-\dim_F t_{\Gamma, \sigma}$. By [1, Prop. A.3], θ_χ is crystalline and $D_{\mathrm{crys}}(\theta_\chi)$ is invertible as a $(K_0 \otimes_{\mathbb{Q}_p} F)$ -module. Extending scalars by $K_0 \rightarrow K$ yields $D_{\mathrm{dR}}(\theta_\chi)$, so the invertibility over $K \otimes_{\mathbb{Q}_p} F$ holds.

It remains to prove that the degree of the σ -isotypic F -line in $\mathrm{gr}^\bullet(D_{\mathrm{dR}}(\theta_\chi))$ is equal to $-\dim_F t_{\Gamma, \sigma}$ for each $\sigma: K \rightarrow F$. Recall that by definition, $\chi: K^\times \rightarrow F^\times$ encodes the K -action on the F -line

$$\det_F(t_\Gamma)^{-1} = \bigotimes_{\sigma: K \rightarrow F} \det_F(t_{\Gamma, \sigma})^{-1}.$$

In other words, for any $c \in K^\times$, $\chi(c) = \prod_\sigma \sigma(c)^{n_\sigma}$ as a product of F^\times -valued characters, i.e. $\theta_\chi = \otimes_\sigma \theta_\sigma^{\otimes n_\sigma}$ where (i) $\theta_\sigma: G_K^{\mathrm{ab}} \rightarrow \mathcal{O}_F^\times$ extends $r_K(u) \mapsto \sigma(u)$ for $u \in \mathcal{O}_K^\times$, and (ii) the tensor product is formed as 1-dimensional F -linear representations. Since we are using covariant Fontaine functors, $D_{\mathrm{dR}}(\theta_\chi) \simeq \otimes_\sigma D_{\mathrm{dR}}(\theta_\sigma)^{\otimes n_\sigma}$ where the tensor product is formed over $K \otimes_{\mathbb{Q}_p} F$ and the definition of the F -linear K -action on the σ -factor via $\sigma: K \rightarrow F$.

By Serre [5, App. III, A.4], the representation θ_σ^{-1} corresponds to the scalar extension along σ of a Lubin–Tate group G_π over \mathcal{O}_K arising from a uniformizer π of K . The associated filtered K -vector space $D_{\mathrm{dR}}(V_p(G_\pi))$ has gr^{-1} of dimension 1 and gr^0 of dimension $[K : \mathbb{Q}_p] - 1$ (since G_π is 1-dimensional p -divisible group of height $[K : \mathbb{Q}_p]$ over \mathcal{O}_K , and $\mathbb{C}_K \otimes D_{\mathrm{dR}} = D_{\mathrm{HT}}$).

Using the G_K -equivariant K -linear structure on $V_p(G_\pi)$, view $D_{\mathrm{dR}}(V_p(G_\pi))$ as a filtered $(K \otimes_{\mathbb{Q}_p} K)$ -module with the left tensor factor encoding the K -linear structure on D_{dR} (arising from B_{dR}) and the right tensor factor encoding the K -action arising from $V_p(G_\pi)$.

Lemma A.4. *As a $(K \otimes_{\mathbb{Q}_p} K)$ -module, $D_{\mathrm{dR}}(V_p(G_\pi))$ is free of rank 1.*

Proof. The comparison isomorphism $B_{\mathrm{dR}} \otimes_K D_{\mathrm{dR}}(V_p(G_\pi)) \simeq B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_p(G_\pi)$ has target that is visibly faithful over $K \otimes_{\mathbb{Q}_p} K$. Hence, $D_{\mathrm{dR}}(V_p(G_\pi))$ is a faithful $(K \otimes_{\mathbb{Q}_p} K)$ -module, so by K -dimension reasons (for the left tensor structure) it is free of rank 1. \square

Using the K -structure for the right tensor factor, $D_{\mathrm{dR}}(\theta_\sigma^{-1}) = D_{\mathrm{dR}}(V_p(G_\pi)) \otimes_{K, \sigma} F$. Thus, by the lemma, $D_{\mathrm{dR}}(\theta_\sigma)$ is an invertible $(K \otimes_{\mathbb{Q}_p} F)$ -module equipped with a linear filtration whose associated graded module is supported in degrees 1 and 0 with the term in degree 1 equal to the σ -isotypic F -line and the term in degree 0 equal to the span of the isotypic F -lines for the other \mathbb{Q}_p -embeddings of K into F . In particular, the $(K \otimes_{\mathbb{Q}_p} F)$ -linear structure canonically splits the filtration (via the decomposition into isotypic F -lines for the K -action), so we may and do view $D_{\mathrm{dR}}(\theta_\sigma)$ as a graded $(K \otimes_{\mathbb{Q}_p} F)$ -module (equipped with the associated tautologous filtration). Hence, $D_{\mathrm{dR}}(\theta_\sigma)^{\otimes n_\sigma}$ is an invertible $(K \otimes_{\mathbb{Q}_p} F)$ -line equipped with a linear grading such that the σ -isotypic F -line is in degree n_σ and

whose other isotypic F -lines are in degree 0 (since the factor rings of $K \otimes_{\mathbb{Q}_p} F$ are pairwise orthogonal).

Finally, the $(K \otimes_{\mathbb{Q}_p} F)$ -linear tensor product over all σ gives that $D_{\mathrm{dR}}(\theta_\chi)$ is an invertible $(K \otimes_{\mathbb{Q}_p} F)$ -module equipped with a linear grading such that its σ -isotypic F -line is the tensor product of the σ -isotypic F -line in $D_{\mathrm{dR}}(\theta_\sigma)^{\otimes n_\sigma}$ (which occurs in degree n_σ) and the σ -isotypic F -lines in the $D_{\mathrm{dR}}(\theta_\tau)^{\otimes n_\tau}$'s for $\tau \neq \sigma$ (which all occur in degree 0). To summarize, for every σ the σ -isotypic F -line in $\mathrm{gr}^\bullet(D_{\mathrm{dR}}(\theta_\chi))$ occurs in degree $n_\sigma = -\dim_F t_{\Gamma, \sigma}$, as desired.

References

- [1] B. Conrad, *Lifting global representations with local properties*, 2010 preprint available at the webpage <http://math.stanford.edu/~conrad/papers/locchar.pdf>.
- [2] B. Conrad, *Semistable reduction for abelian varieties*, seminar lecture notes available at the webpage <http://math.stanford.edu/~akshay/ntslearn.html>.
- [3] J-M. Fontaine, “Le corps des périodes p -adiques” in *Périodes p -adiques*, Astérisque 223 (1994), pp. 59–111.
- [4] J-M. Fontaine, “Représentations p -adiques semi-stables” in *Périodes p -adiques*, Astérisque 223 (1994), pp. 113–184.
- [5] J-P. Serre, *Abelian ℓ -adic representations and elliptic curves* (2nd ed.), A.K. Peters, 1998.